

S01P1590US00

日 本 国 特 許 庁
JAPAN PATENT OFFICE

11036 U.S. PTO
09/982624
10/18/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年10月20日

出 願 番 号

Application Number:

特願2000-320805

出 願 人

Applicant(s):

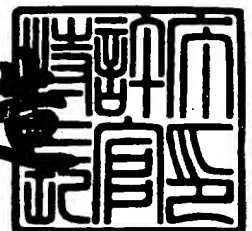
ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 8月31日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



【書類名】 特許願

【整理番号】 0000647705

【提出日】 平成12年10月20日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 13/00

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 白井 太三

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 石橋 義人

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 吉野 賢治

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 秋下 徹

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100101801

【弁理士】

【氏名又は名称】 山田 英治

【電話番号】 03-5541-7577

【選任した代理人】

【識別番号】 100093241

【弁理士】

【氏名又は名称】 宮田 正昭

【電話番号】 03-5541-7577

【選任した代理人】

【識別番号】 100086531

【弁理士】

【氏名又は名称】 澤田 俊夫

【電話番号】 03-5541-7577

【手数料の表示】

【予納台帳番号】 062721

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9904833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ記憶装置、およびデータ記録方法、データ再生方法、並びにプログラム提供媒体

【特許請求の範囲】

【請求項 1】

各々が予め定められたデータ容量を持つ複数のセクタを 1 ブロックとしたブロックを複数有するデータ格納領域と、暗号処理手段とを有するデータ記憶装置において、

前記暗号処理手段は、

前記データ記憶装置とデータ通信可能なデバイスから、前記データ格納領域に格納するデータの暗号処理鍵として、前記複数のセクタ各々の暗号処理用鍵または復号処理用鍵として対応づけられた複数の鍵からなる鍵セットを受領し、該受領した鍵セットに対して CBC モードでの暗号処理を実行して、前記デバイスに送信する処理を実行する構成を有することを特徴とするデータ記憶装置。

【請求項 2】

前記暗号処理手段は、

前記鍵セットに対する CBC モードでの暗号処理を、前記データ記憶装置に固有の保存鍵 K_{sto} を適用して実行して前記データ格納領域に格納するデータのヘッダ情報としての鍵データを生成する構成を有することを特徴とする請求項 1 に記載のデータ記憶装置。

【請求項 3】

前記データ記憶装置は、

前記データ記憶装置とデータ通信可能な前記デバイスとの相互認証処理を実行する構成を有し、

前記デバイスから受領する鍵セットは、前記相互認証時に生成したセッション鍵を用いた CBC モードによる暗号化を行なったセッション鍵適用 CBC モード処理鍵セットであり、

前記暗号処理手段は、

前記セッション鍵適用 CBC モード処理鍵セットを前記セッション鍵を用いた

CBCモードで復号し、

復号した鍵セットを前記データ記憶装置に固有の保存鍵K s t oに基づいてCBCモードで暗号処理を実行して、保存鍵適用CBCモード処理鍵セットを生成して前記デバイスにヘッダ情報構成データとして送信する処理を実行する構成を有することを特徴とする請求項1に記載のデータ記憶装置。

【請求項4】

前記データ記憶装置は、

前記データ記憶装置とデータ通信可能な前記デバイスとの相互認証処理を実行する構成を有し、

前記デバイスから受領する鍵セットは、前記データ格納領域に格納するデータのヘッダ情報として格納された鍵セットであって、前記データ記憶装置に固有の保存鍵K s t oに基づいてCBCモードで暗号処理を実行した保存鍵適用CBCモード処理鍵セットであり、

前記暗号処理手段は、

前記保存鍵適用CBCモード処理鍵セットを保存鍵を用いたCBCモードで復号し、

復号した鍵セットを前記相互認証時に生成したセッション鍵に基づいてCBCモードで暗号処理を実行して、セッション鍵適用CBCモード処理鍵セットを生成して前記デバイスにデータ復号用鍵情報構成データとして送信する処理を実行する構成を有することを特徴とする請求項1に記載のデータ記憶装置。

【請求項5】

前記暗号処理手段は、

前記データ記憶装置とデータ通信可能なデバイスから、前記データ格納領域に格納するデータの暗号処理鍵として、前記複数のセクタ各々の暗号処理用鍵または復号処理用鍵として対応づけられた複数の鍵からなる鍵セットと、

前記複数のセクタの少なくともいずれかに格納されるデータの改竄チェック値(I C V)生成用の鍵K i c vと、

を受領し、該受領した鍵セットに対してCBCモードでの暗号処理を実行して、前記デバイスに送信する処理を実行する構成を有することを特徴とする請求項

1 に記載のデータ記憶装置。

【請求項 6】

各々が予め定められたデータ容量を持つ複数のセクタを 1 ブロックとしたブロックを複数有するデータ格納領域と、暗号処理手段とを有するデータ記憶装置と

該データ記憶装置にデータを送信してデータの格納処理を実行するデータ記録装置とを有するデータ処理装置におけるデータ記録方法において、

前記データ記憶装置および前記データ記録装置間において相互認証処理を実行するステップと、

前記相互認証の成立を条件として、前記データ記録装置において、前記複数のセクタ各々の格納データの暗号処理に適用する複数の暗号鍵からなる暗号鍵セットを前記相互認証時に生成したセッション鍵を用いた CBC モードによって暗号化して、セッション鍵適用 CBC モード処理鍵セットを生成して、前記データ記憶装置に対して送信するステップと、

前記データ記憶装置において、前記セッション鍵適用 CBC モード処理鍵セットをセッション鍵を適用した CBC モードで復号するステップと、

復号した鍵セットを前記データ記憶装置に固有の保存鍵 *K s t o* に基づいて CBC モードで暗号化して、保存鍵適用 CBC モード処理鍵セットを生成して、前記データ記録装置に送信するステップと、

前記データ記録装置において、前記データ記憶装置に格納するデータに対応するヘッダ情報として、受信した前記保存鍵適用 CBC モード処理鍵セットデータを構成要素として含むヘッダ情報を生成するステップと、

を有することを特徴とするデータ記録方法。

【請求項 7】

各々が予め定められたデータ容量を持つ複数のセクタを 1 ブロックとしたブロックを複数有するデータ格納領域と、暗号処理手段とを有するデータ記憶装置と

該データ記憶装置からデータを受信してデータの再生処理を実行するデータ再生装置とを有するデータ処理装置におけるデータ再生方法において、

前記データ記憶装置および前記データ再生装置間において相互認証処理を実行するステップと、

前記相互認証の成立を条件として、前記データ格納領域に格納されたデータのヘッダ情報に含まれる鍵セットであって、前記データ記憶装置に固有の保存鍵 K_{sto} に基づいて CBC モードで暗号処理を実行した保存鍵適用 CBC モード処理鍵セットを前記データ記録装置から前記データ記憶装置に送信するステップと

前記データ記憶装置において、

前記保存鍵適用 CBC モード処理鍵セットを保存鍵を用いた CBC モードで復号するステップと、

復号した鍵セットを前記相互認証時に生成したセッション鍵に基づいて CBC モードで暗号処理を実行して、セッション鍵適用 CBC モード処理鍵セットを生成して前記データ再生装置に送信するステップと、

前記データ再生装置において、前記セッション鍵適用 CBC モード処理鍵セットをセッション鍵を適用した CBC モードにより復号して、前記データ格納領域の各セクタに格納された暗号化セクタデータの復号用の鍵セットを取得するステップと、

を有することを特徴とするデータ再生方法。

【請求項 8】

各々が予め定められたデータ容量を持つ複数のセクタを 1 ブロックとしたブロックを複数有するデータ格納領域と、暗号処理手段とを有するデータ記憶装置と

該データ記憶装置にデータを送信してデータの格納処理を実行するデータ記録装置とを有するデータ処理装置におけるデータ記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

前記データ記憶装置および前記データ記録装置間において相互認証処理を実行するステップと、

前記相互認証の成立を条件として、前記データ記録装置において、前記複数の

セクタ各々の格納データの暗号処理に適用する複数の暗号鍵からなる暗号鍵セットを前記相互認証時に生成したセッション鍵を用いたCBCモードによって暗号化して、セッション鍵適用CBCモード処理鍵セットを生成して、前記データ記憶装置に対して送信するステップと、

前記データ記憶装置において、前記セッション鍵適用CBCモード処理鍵セットをセッション鍵を適用したCBCモードで復号するステップと、

復号した鍵セットを前記データ記憶装置に固有の保存鍵K_{sto}に基づいてCBCモードで暗号化して、保存鍵適用CBCモード処理鍵セットを生成して、前記データ記録装置に送信するステップと、

前記データ記録装置において、前記データ記憶装置に格納するデータに対応するヘッダ情報として、受信した前記保存鍵適用CBCモード処理鍵セットデータを構成要素として含むヘッダ情報を生成するステップと、

を有することを特徴とするプログラム提供媒体。

【請求項 9】

各々が予め定められたデータ容量を持つ複数のセクタを1ブロックとしたブロックを複数有するデータ格納領域と、暗号処理手段とを有するデータ記憶装置と

該データ記憶装置からデータを受信してデータの再生処理を実行するデータ再生装置とを有するデータ処理装置におけるデータ再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

前記データ記憶装置および前記データ再生装置間において相互認証処理を実行するステップと、

前記相互認証の成立を条件として、前記データ格納領域に格納されたデータのヘッダ情報に含まれる鍵セットであって、前記データ記憶装置に固有の保存鍵K_{sto}に基づいてCBCモードで暗号処理を実行した保存鍵適用CBCモード処理鍵セットを前記データ記録装置から前記データ記憶装置に送信するステップと

前記データ記憶装置において、

前記保存鍵適用CBCモード処理鍵セットを保存鍵を用いたCBCモードで復号するステップと、

復号した鍵セットを前記相互認証時に生成したセッション鍵に基づいてCBCモードで暗号処理を実行して、セッション鍵適用CBCモード処理鍵セットを生成して前記データ再生装置に送信するステップと、

前記データ再生装置において、前記セッション鍵適用CBCモード処理鍵セットをセッション鍵を適用したCBCモードにより復号して、前記データ格納領域の各セクタに格納された暗号化セクタデータの復号用の鍵セットを取得するステップと、

を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、データ記憶装置、およびデータ記録方法、データ再生方法、並びにプログラム提供媒体に関する。特に、記憶装置に格納されるコンテンツを高度なセキュリティ管理のもとに保護することを可能とするデータ記憶装置、およびデータ記録方法、データ再生方法、並びにプログラム提供媒体に関する。

【0002】

【従来の技術】

近年のインターネットの急激な普及、さらにモバイル型の小型再生器、ゲーム器等の普及に伴い、音楽データ、ゲームプログラム、画像データ等、様々なソフトデータ（以下、これらをコンテンツ（Content）と呼ぶ）の、インターネット等のネットワーク、あるいは、DVD、CD、メモリカード等の記憶媒体を介した流通が急増している。これらの流通コンテンツは、ユーザの所有するPC（Personal Computer）、再生専用器、あるいはゲーム機器においてネットワークから受信され記憶媒体に格納されたり、あるいはコンテンツを格納したメモリカード、CD、DVD等の記憶媒体を再生専用器、あるいはゲーム機器に装着することにより、コンテンツ再生処理、あるいはプログラム実行が可能となる。

【0003】

コンテンツの記憶素子として、最近多く利用される素子にフラッシュメモリがある。フラッシュメモリは、EEPROM(Electrically Erasable Programmable ROM)と呼ばれる電氣的に書き換え可能な不揮発性メモリの一形態である。従来のEEPROMは、1ビットを2個のトランジスタで構成するために、1ビット当たりの占有面積が大きく、集積度を高くするのに限界があったが、フラッシュメモリは、全ビット一括消去方式により1ビットを1トランジスタで実現することが可能となった。フラッシュメモリは、磁気ディスク、光ディスク等の記録媒体に代わりうるものとして期待されている。

【0004】

フラッシュメモリをデータ記録／再生機器に対して着脱自在に構成したメモリカードも知られている。このメモリカードを使用すれば、従来のCD（コンパクトディスク：登録商標）、MD（ミニディスク：登録商標）等のディスク状媒体に換えてメモリカードを使用するデジタルオーディオ記録／再生装置を実現することができる。

【0005】

このような、フラッシュメモリを使用したコンテンツ記憶素子をパーソナルコンピュータ（PC）、再生器等において使用する場合、FAT(File Allocation Table)システムと呼ばれるファイル管理システムがアクセス情報テーブルとして一般的に使用される。FATシステムでは、必要なファイルが定義されると、その中に必要なパラメータがファイルの先頭から順番にセットされる。その結果、ファイルサイズを可変長とすることができ、1ファイルを1または複数の管理単位（セクタ、クラスタ等）で構成することができる。この管理単位の関連事項がFATと呼ばれるテーブルに書かれる。このFATシステムは、記録媒体の物理的特性と無関係に、ファイル構造を容易に構築することができる。従って、FATシステムは、フロッピーディスク、ハードディスクのみならず、光磁気ディスクにおいても採用することができる。上述したメモリカードにおいても、FATシステムが採用されている。

【0006】

音楽データ、画像データ、あるいはプログラム等の様々なコンテンツは、再生

機器として利用される再生装置、ゲーム機器、P C等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により、上述のF A Tに基づいて例えば上述したフラッシュメモリから呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

【0 0 0 7】

さらに、ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規のユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

【0 0 0 8】

ユーザに対する利用制限を実現する1つの手法が、配布コンテンツの暗号化処理である。すなわち、例えばインターネット等を介して暗号化された音声データ、画像データ、ゲームプログラム等の各種コンテンツを配布するとともに、正規ユーザであると確認された者に対してのみ、配布された暗号化コンテンツを復号する手段、すなわち復号鍵を付与する構成である。

【0 0 0 9】

暗号化データは、所定の手続きによる復号処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号処理に復号鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

【0 0 1 0】

【発明が解決しようとする課題】

例えばメモリ上にコンテンツを格納する場合、著作権などを保護するためにコンテンツ部に対する暗号化を行う場合があるが、コンテンツ部全体に対して一つの暗号化鍵を使って暗号化すると、同一の鍵のみに基づく大量の暗号文が発生し、攻撃が容易となってしまう危険性がある。コンテンツ部をできるだけ分割し、それぞれを異なる鍵で暗号化する方が望ましいと言える。コンテンツ暗号化の最

小単位として、セクタが挙げられる。

【0011】

一方、複数のコンテンツ暗号鍵を安全に格納するための構成が問題となる。本発明は、コンテンツの暗号化等に適用する複数の鍵を安全に、すなわち、セキュリティを高めて保持することを可能としたデータ記憶装置、およびデータ記録方法、データ再生方法、並びにプログラム提供媒体を提供することを目的とする。

【0012】

具体的には、本発明は、各コンテンツの属性情報であるヘッダの中に例えば、メディアの1ブロックあたりのセクタ数Mに対応するM個の鍵情報を暗号化して格納し、これらの暗号化処理をよりセキュリティの高い暗号化モードで実行する構成とすることにより、セキュリティを高い鍵保管を可能としたデータ記憶装置、およびデータ記録方法、データ再生方法、並びにプログラム提供媒体を提供する。

【0013】

【課題を解決するための手段】

本発明の第1の側面は、

各々が予め定められたデータ容量を持つ複数のセクタを1ブロックとしたブロックを複数有するデータ格納領域と、暗号処理手段とを有するデータ記憶装置において、

前記暗号処理手段は、

前記データ記憶装置とデータ通信可能なデバイスから、前記データ格納領域に格納するデータの暗号処理鍵として、前記複数のセクタ各々の暗号処理用鍵または復号処理用鍵として対応づけられた複数の鍵からなる鍵セットを受領し、該受領した鍵セットに対してCBCモードでの暗号処理を実行して、前記デバイスに送信する処理を実行する構成を有することを特徴とするデータ記憶装置にある。

【0014】

さらに、本発明のデータ記憶装置の一実施態様において、前記暗号処理手段は、前記鍵セットに対するCBCモードでの暗号処理を、前記データ記憶装置に固有の保存鍵 K_{sto} を適用して実行して前記データ格納領域に格納するデータの

ヘッダ情報としての鍵データを生成する構成を有することを特徴とする。

【0015】

さらに、本発明のデータ記憶装置の一実施態様において、前記データ記憶装置は、前記データ記憶装置とデータ通信可能な前記デバイスとの相互認証処理を実行する構成を有し、前記デバイスから受領する鍵セットは、前記相互認証時に生成したセッション鍵を用いたCBCモードによる暗号化を行なったセッション鍵適用CBCモード処理鍵セットであり、前記暗号処理手段は、前記セッション鍵適用CBCモード処理鍵セットを前記セッション鍵を用いたCBCモードで復号し、復号した鍵セットを前記データ記憶装置に固有の保存鍵K_{sto}に基づいてCBCモードで暗号処理を実行して、保存鍵適用CBCモード処理鍵セットを生成して前記デバイスにヘッダ情報構成データとして送信する処理を実行する構成を有することを特徴とする。

【0016】

さらに、本発明のデータ記憶装置の一実施態様において、前記データ記憶装置は、前記データ記憶装置とデータ通信可能な前記デバイスとの相互認証処理を実行する構成を有し、前記デバイスから受領する鍵セットは、前記データ格納領域に格納するデータのヘッダ情報として格納された鍵セットであって、前記データ記憶装置に固有の保存鍵K_{sto}に基づいてCBCモードで暗号処理を実行した保存鍵適用CBCモード処理鍵セットであり、前記暗号処理手段は、前記保存鍵適用CBCモード処理鍵セットを保存鍵を用いたCBCモードで復号し、復号した鍵セットを前記相互認証時に生成したセッション鍵に基づいてCBCモードで暗号処理を実行して、セッション鍵適用CBCモード処理鍵セットを生成して前記デバイスにデータ復号用鍵情報構成データとして送信する処理を実行する構成を有することを特徴とする。

【0017】

さらに、本発明のデータ記憶装置の一実施態様において、前記暗号処理手段は、前記データ記憶装置とデータ通信可能なデバイスから、前記データ格納領域に格納するデータの暗号処理鍵として、前記複数のセクタ各々の暗号処理用鍵または復号処理用鍵として対応づけられた複数の鍵からなる鍵セットと、前記複数の

セクタの少なくともいずれかに格納されるデータの改竄チェック値（ICV）生成用の鍵 K_{icv} と、を受領し、該受領した鍵セットに対してCBCモードでの暗号処理を実行して、前記デバイスに送信する処理を実行する構成を有することを特徴とする。

【0018】

さらに、本発明の第2の側面は、

各々が予め定められたデータ容量を持つ複数のセクタを1ブロックとしたブロックを複数有するデータ格納領域と、暗号処理手段とを有するデータ記憶装置と

該データ記憶装置にデータを送信してデータの格納処理を実行するデータ記録装置とを有するデータ処理装置におけるデータ記録方法において、

前記データ記憶装置および前記データ記録装置間において相互認証処理を実行するステップと、

前記相互認証の成立を条件として、前記データ記録装置において、前記複数のセクタ各々の格納データの暗号処理に適用する複数の暗号鍵からなる暗号鍵セットを前記相互認証時に生成したセッション鍵を用いたCBCモードによって暗号化して、セッション鍵適用CBCモード処理鍵セットを生成して、前記データ記憶装置に対して送信するステップと、

前記データ記憶装置において、前記セッション鍵適用CBCモード処理鍵セットをセッション鍵を適用したCBCモードで復号するステップと、

復号した鍵セットを前記データ記憶装置に固有の保存鍵 K_{sto} に基づいてCBCモードで暗号化して、保存鍵適用CBCモード処理鍵セットを生成して、前記データ記録装置に送信するステップと、

前記データ記録装置において、前記データ記憶装置に格納するデータに対応するヘッダ情報として、受信した前記保存鍵適用CBCモード処理鍵セットデータを構成要素として含むヘッダ情報を生成するステップと、

を有することを特徴とするデータ記録方法にある。

【0019】

さらに、本発明の第3の側面は、

各々が予め定められたデータ容量を持つ複数のセクタを1ブロックとしたブロックを複数有するデータ格納領域と、暗号処理手段とを有するデータ記憶装置と

該データ記憶装置からデータを受信してデータの再生処理を実行するデータ再生装置とを有するデータ処理装置におけるデータ再生方法において、

前記データ記憶装置および前記データ再生装置間において相互認証処理を実行するステップと、

前記相互認証の成立を条件として、前記データ格納領域に格納されたデータのヘッダ情報に含まれる鍵セットであって、前記データ記憶装置に固有の保存鍵 K_{sto} に基づいてCBCモードで暗号処理を実行した保存鍵適用CBCモード処理鍵セットを前記データ記録装置から前記データ記憶装置に送信するステップと

前記データ記憶装置において、

前記保存鍵適用CBCモード処理鍵セットを保存鍵を用いたCBCモードで復号するステップと、

復号した鍵セットを前記相互認証時に生成したセッション鍵に基づいてCBCモードで暗号処理を実行して、セッション鍵適用CBCモード処理鍵セットを生成して前記データ再生装置に送信するステップと、

前記データ再生装置において、前記セッション鍵適用CBCモード処理鍵セットをセッション鍵を適用したCBCモードにより復号して、前記データ格納領域の各セクタに格納された暗号化セクタデータの復号用の鍵セットを取得するステップと、

を有することを特徴とするデータ再生方法にある。

【0020】

さらに、本発明の第4の側面は、

各々が予め定められたデータ容量を持つ複数のセクタを1ブロックとしたブロックを複数有するデータ格納領域と、暗号処理手段とを有するデータ記憶装置と

該データ記憶装置にデータを送信してデータの格納処理を実行するデータ記録

装置とを有するデータ処理装置におけるデータ記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

前記データ記憶装置および前記データ記録装置間において相互認証処理を実行するステップと、

前記相互認証の成立を条件として、前記データ記録装置において、前記複数のセクタ各々の格納データの暗号処理に適用する複数の暗号鍵からなる暗号鍵セットを前記相互認証時に生成したセッション鍵を用いたCBCモードによって暗号化して、セッション鍵適用CBCモード処理鍵セットを生成して、前記データ記憶装置に対して送信するステップと、

前記データ記憶装置において、前記セッション鍵適用CBCモード処理鍵セットをセッション鍵を適用したCBCモードで復号するステップと、

復号した鍵セットを前記データ記憶装置に固有の保存鍵Kst oに基づいてCBCモードで暗号化して、保存鍵適用CBCモード処理鍵セットを生成して、前記データ記録装置に送信するステップと、

前記データ記録装置において、前記データ記憶装置に格納するデータに対応するヘッダ情報として、受信した前記保存鍵適用CBCモード処理鍵セットデータを構成要素として含むヘッダ情報を生成するステップと、

を有することを特徴とするプログラム提供媒体にある。

【0021】

さらに、本発明の第5の側面は、

各々が予め定められたデータ容量を持つ複数のセクタを1ブロックとしたブロックを複数有するデータ格納領域と、暗号処理手段とを有するデータ記憶装置と

、
該データ記憶装置からデータを受信してデータの再生処理を実行するデータ再生装置とを有するデータ処理装置におけるデータ再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

前記データ記憶装置および前記データ再生装置間において相互認証処理を実行

するステップと、

前記相互認証の成立を条件として、前記データ格納領域に格納されたデータのヘッダ情報に含まれる鍵セットであって、前記データ記憶装置に固有の保存鍵 K_{sto} に基づいて CBC モードで暗号処理を実行した保存鍵適用 CBC モード処理鍵セットを前記データ記録装置から前記データ記憶装置に送信するステップと

前記データ記憶装置において、

前記保存鍵適用 CBC モード処理鍵セットを保存鍵を用いた CBC モードで復号するステップと、

復号した鍵セットを前記相互認証時に生成したセッション鍵に基づいて CBC モードで暗号処理を実行して、セッション鍵適用 CBC モード処理鍵セットを生成して前記データ再生装置に送信するステップと、

前記データ再生装置において、前記セッション鍵適用 CBC モード処理鍵セットをセッション鍵を適用した CBC モードにより復号して、前記データ格納領域の各セクタに格納された暗号化セクタデータの復号用の鍵セットを取得するステップと、

を有することを特徴とするプログラム提供媒体にある。

【 0 0 2 2 】

なお、本発明の第 4、5 の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CD や FD、MO などの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【 0 0 2 3 】

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され

、本発明の他の側面と同様の作用効果を得ることができるのである。

【 0 0 2 4 】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【 0 0 2 5 】

【発明の実施の形態】

〔システム概要〕

図1に本発明のデータ処理装置の適用可能なコンテンツ配信システム構成を示す。例えば音楽データ、画像データ、その他各種プログラム等のコンテンツが、コンテンツ保持者またはサービスプロバイダのようなシステム運営者101から、インターネット等のネットワークを介して、またはCD、DVD、フラッシュメモリを搭載したメモリカード等の各種記録媒体であるメディア103に格納され、デバイス102に受信または装着されて再生、実行される。デバイスは、例えばパーソナルコンピュータ（PC）、再生専用器、ゲーム器等のコンテンツ再生機能を有するデバイスであり、例えば画像コンテンツを表示する表示装置、ユーザの指示を入力する入力装置を有する。

【 0 0 2 6 】

このようなコンテンツ配信システムの構成中、コンテンツを再生するデバイスと、コンテンツを格納するメディアとの詳細構成を図2に示す。

【 0 0 2 7 】

図2は、デバイス200、メディア1、210、メディア2、230の詳細構成を示している。メディア1、210は、単純なデータ読み出し、書き込み処理のみをサポートする制御部を持つメディアであり、メディア2、230は、メディアを装着するデバイスとの相互認証処理を実行し、またメディアに格納するコンテンツの暗号処理を実行するコントローラを有するメディアである。メディア1、210、メディア2、230の双方ともデバイス200に対する装着が可能である。

【 0 0 2 8 】

図2のデバイス200は、インターネット等のデータ通信手段を介したデータ

送受信処理を実行する通信部 2 0 1、各種指示を入力する入力部 2 0 2、メッセージ、コンテンツ等の表示を実行する表示部 2 0 3、これらの制御を実行する制御部 2 0 5 と、メディアとのデータ入出力処理のインタフェース機能を持つメモリインタフェース (I/F) 部 3 0 0 とを持つデバイスコントローラ 2 0 4、さらに、コンテンツのファイル群と、不正なメディアやコンテンツの失効情報としてのリボケーションリストを格納している内部メモリとしてのメモリ部 2 0 7 を有する。なお、内部メモリ内に格納されるリボケーションリスト等のデータファイルは、ファイル割り当てテーブルによって管理され読み出し可能な構成を持つ。

【 0 0 2 9 】

デバイス 2 0 0 は、コンテンツの再生時に再生対象のコンテンツがリボケーションリストに格納された失効メディア、失効コンテンツに対応していないことを確認した上で再生を行なう。再生対象のコンテンツがリボケーションリストにリストアップされていた場合は、再生エラーとなり、再生処理が実行されない。リボケーションリスト、およびリボケーションリストを適用した再生処理については後段で詳細に説明する。

【 0 0 3 0 】

メディア 1, 2 1 0 は、データ入出力を制御する制御部 2 1 1 と、コンテンツを格納するメモリ部 2 1 2 を有し、メモリ部 2 1 2 は、コンテンツを対応ヘッダ情報とともに格納するのみならず、メディア個々に固有の識別情報としてのメディア ID、さらに、メモリアクセスコントロール情報を記述したアクセス許可テーブルである BPT (Block Permission Table) を格納している。

【 0 0 3 1 】

デバイス 2 0 0 のファイルシステムはメディアを認識した後に、アクセス許可テーブルである BPT をメディアから読み込み、メディアへ直接アクセスを行うメモリインターフェイス部 3 0 0 に BPT を転送し、管理させる。メモリインターフェイス部 3 0 0 は、BPT を受信した後、受信した BPT について改竄チェック値 (ICV) の検証を行う。ICV が正当なものと判断された場合のみ、BPT を有効なものとして保存する。メモリインターフェイス部 3 0 0 は、メディ

アのメモリにアクセスする命令を受信した時、このメディアのBPTに基づいたアクセスのみ実行する。BPTの構成、およびBPTを用いた処理に関しては後段で詳細に説明する。

【0032】

メディア2, 230は、コントローラ231と、メモリ部232によって構成され、メモリ部232は、コンテンツを対応ヘッダ情報とともに格納し、さらにアクセス許可テーブルであるBPT (Block Permission Table) を格納している。コントローラ231は、メモリ部232に対するデータ格納、またはデータ読み出し用インタフェースとしてのメモリアンタフェース(I/F)部234、メディアの識別子としてのメディア2ID、相互認証処理に適用する認証鍵Kake、コンテンツのメモリ部232への保存時の暗号鍵である保存鍵Ksto、さらに暗号化対象の鍵を暗号化する時の初期値IV_key等格納した内部メモリ235、認証処理あるいはコンテンツの暗号化、復号処理を実行し、レジスタを備えた暗号処理部236、そして、これら各部の制御を実行する制御部233とを有する。

【0033】

【メディア内メモリ構成】

次に、メディア1, 210、メディア2, 230の各メモリ部のデータ格納構成を図3に示す。メモリ部は例えば、EEPROM(Electrically Erasable Programmable ROM)と呼ばれる電氣的に書き換え可能な不揮発性メモリの一形態であるフラッシュメモリであり、ブロック単位の一括消去方式によるデータ消去が実行される。

【0034】

図3(a)に示すように、フラッシュメモリは、第1~Nまでの複数ブロックを有し、各ブロックは、(b)に示すように第1~Mまでの複数セクタによって構成され、各セクタは(c)に示すように実データを含むデータ部と、エラー訂正コード等の冗長データを含む冗長部によって構成される。後段で詳細に説明するが、冗長部には各セクタのデータ部内のセクタデータ改竄チェック値としてのICVが格納される場合がある。

【0035】

〔主要コマンド〕

次に図2のデバイス200において、制御部205と、メモリーインターフェース（I/F）部300において発行される主なコマンドについて説明する。

【0036】

まず、制御部205からメモリーインターフェース（I/F）部300に対するコマンドには、以下のものがある。

・ステータス読み出しコマンド

現在のメモリーインターフェース内のステータスを設定したステータスレジスタの状態の読み出し。メモリーインターフェース（I/F）部300は、ステータスレジスタの内容を返す。

・セクタ読み出しコマンド

指定したセクタのデータ読み出し処理命令。

・セクタ書き込みコマンド

指定したセクタへのデータ書き込み処理命令。

・セクタ復号読み出しコマンド

セットされたヘッダの情報を元に、指定されたセクタの暗号化データを復号して読み出す処理の実行命令。

・セクタ暗号書き込みコマンド

セットされたヘッダの情報を元に、指定されたセクタへデータを暗号化して書き込む処理の実行命令。

・ヘッダ生成コマンド

指定されたパラメータを元にヘッダを生成する処理の実行命令。

・ヘッダセットコマンド

ヘッダをメモリーインターフェース内にセットする処理の実行命令。

・BPTセットコマンド

BPTをメモリーインターフェース内にセットする処理の実行命令。

・リボケーションリスト（Revocation List）セットコマンド

不正メディア、不正コンテンツのリストであるリボケーションリスト（Revoca

tion List) をメモリーインターフェイス内にセットする処理の実行命令。

- ・更新用リボケーションリスト (Revocation List) チェックコマンド

更新用リボケーションリスト (Revocation List) に現在のリボケーションリスト (Revocation List) を更新してよいかチェックする処理の実行命令。

- ・メディア 1 認識コマンド

接続されたメディア 1 に対してメディアの識別子 (I D) を読み出して、その I D が有効かどうかチェックする処理の実行命令。

- ・メディア 2 認識コマンド

接続されたメディア 2 に対して相互認証をして、メディアの識別子 (I D) が有効かどうかチェックする処理の実行命令。

- ・ファイル割り当てテーブル呼び出しコマンド

メモリ内のファイル割り当てテーブルを読み出す処理の実行命令。

- ・ファイル割り当てテーブル更新コマンド

メモリへのファイル割り当てテーブルを更新する処理の実行命令。

【 0 0 3 7 】

メモリーインターフェイス (I / F) 部 3 0 0 からメディア 1 に対するコマンドは、以下のものがある。

- ・ I D 読み出しコマンド

メディア 1 の持つ I D を読み出す処理の実行命令。

【 0 0 3 8 】

[デバイス内メモリーインタフェース詳細構成]

次にデバイス 2 0 0 のメモリーインタフェース (I / F) 部 3 0 0 の詳細構成を図 4 に示す。各構成部の機能を説明する。

【 0 0 3 9 】

- ・ステータスレジスタ 3 0 1

メモリーインターフェイスの内部ステータスを保存するレジスタである。ステータスレジスタ 3 0 1 の構成例を図 5 に示す。各ビットは以下の意味を持つ。

- ・ビット 0 (bit 0) : ビジーフラグ (1 : ビジー (busy) , 0 : 待機 (ready))

メモリインターフェイスが内部処理をしているかの判別用ビットである。

- ・ビット 1 (bit 1) : 読み出し成功フラグ (1: 成功 (success), 0: 失敗 (fail))

メモリからデータの読み出しが成功したかの判別用ビットである。

- ・ビット 2 (bit 2) : 書き込み成功フラグ (1: 成功 (success), 0: 失敗 (fail))

メモリヘデータの書き込みが成功したかの判別用ビットである。

- ・ビット 3 (bit 3) : メディア 1 セットフラグ (1: セット (set), 0: 未セット (not set))

接続されたメディア 1 が利用可能かの判別用ビットである。

- ・ビット 4 (bit 4) : メディア 2 セットフラグ (1: セット (set), 0: 未セット (not set))

接続されたメディア 2 が利用可能かの判別用ビットである。

- ・ビット 5 (bit 5) : メディア 1 有効フラグ (1: 有効 (OK), 0: 無効 (NG))

接続されたメディア 1 の識別子 (ID) が、リボケーションリスト (Revocation List) 内のリボーク (排除) メディア対象外かの判別用ビットである。

- ・ビット 6 (bit 6) : メディア 2 有効フラグ (1: 有効 (OK), 0: 無効 (NG))

接続されたメディア 2 の識別子 (ID) が、リボケーションリスト (Revocation List) 内のリボーク (排除) メディア対象外かの判別用ビットである。

- ・ビット 7 (bit 7) : ヘッダセット成功フラグ (1: 成功 (success), 0: 失敗 (fail))

ヘッダがメモリインターフェイス内にセット出来たかの判別用ビットである。

- ・ビット 8 (bit 8) : ヘッダ生成成功フラグ (1: 成功 (success), 0: 失敗 (fail))

ヘッダの生成が成功したかの判別用ビットである。

- ・ビット 9 (bit 9) : リボケーションリスト (Revocation List) セットフラグ (1: セット (set), 0: 未セット (not set))

リボケーションリスト (Revocation List) がメモリインターフェイス内にセット出来たかの判別用ビットである。

- ・ビット 10 (bit 10) : 更新用リボケーションリスト (Revocation List) 有効フラグ (1: 有効 (OK), 0: 無効 (NG))

更新用リボケーションリスト (Revocation List) が有効であるかどうかの判別用ビットである。

【0040】

ステータスレジスタ 301 は、これらのインタフェース (I/F) 部 300 のステータス情報を保持する。

【0041】

図4に戻り、各構成の機能について説明を続ける。

- ・コマンドレジスタ 302

制御部より送信されたコマンドを保存するレジスタ

- ・アドレスレジスタ 303

データの転送開始セクタを設定するレジスタ

- ・カウントレジスタ 304

データの全転送セクタ数を設定するレジスタ

【0042】

なお、外部メモリ、内部メモリに対するデータの読み書きは、アドレスレジスタに読み書きを開始するセクタアドレスを設定し、カウントレジスタに読み書きをする総セクタ数を設定し、コマンドレジスタにセクタ読み書きコマンドをセットすることで実行される。

【0043】

- ・コントロールレジスタ 305

メモリインターフェイスの動作を設定するレジスタ

- ・送受信制御部 306

各種レジスタおよび送受信バッファなど、メモリインターフェイスの制御を行う。

- ・送信バッファメモリ 307

送信データを格納するバッファ

- ・受信バッファメモリ308

受信データを格納するバッファ

- ・送信レジスタ309

送信バッファメモリ307内のデータを送信するためのレジスタ

- ・受信レジスタ310

受信したデータを保存し受信バッファメモリ308に転送するためのレジスタ
【0044】

- ・暗号処理部320

送信バッファメモリ307、受信バッファメモリ308内のデータに対して、各種暗号処理を施す。

- ・メモリ部321

暗号処理部320における暗号処理に必要な鍵情報、および内部メモリから読み込まれるリボケーションリスト、外部メモリから読み込まれるアクセス許可テーブルとしてのブロック・パーミッション・テーブル（BPT）を格納、保存する領域である。リボケーションリスト、ブロック・パーミッション・テーブル（BPT）それぞれがメモリインタフェース内に有効にセットされた場合、送受信制御部306が制御部からのメディア認識コマンド、あるいは外部メモリに対するデータの読み書きコマンド等を受信した場合、セットされたりボケーションリスト、ブロック・パーミッション・テーブル（BPT）を参照した処理が実行される。これらの処理については、後段でフローを用いて詳細に説明する。

【0045】

さらに、メモリ部321には、暗号処理に必要な鍵情報としては、以下のデータが格納される。

Kdist：メディア2に格納されるコンテンツ以外のコンテンツのセキュリティヘッダ（Security Header）に含まれる配送鍵。コンテンツICV生成鍵Kicv_cont、コンテンツ鍵Kcを暗号化する。

Kicv_sh：セキュリティヘッダ（Security Header）のICVを生成する際に用いるセキュリティヘッダICV生成鍵。

IVsh: セキュリティヘッダ (Security Header) のICVを生成する際に用いる初期値 (IV: Initial Value)。

MKake: 相互認証用のマスター鍵。

IVake: 相互認証用の鍵の生成処理に適用するための初期値 (IV: Initial Value)。

IVauth: 相互認証時のデータ生成用の初期値 (IV: Initial Value)。

MKicv_rl: リボケーションリスト (Revocation List) のICV鍵を生成するマスター鍵。

IVicv_rl: リボケーションリスト (Revocation List) のICV鍵を生成する時の初期値 (IV: Initial Value)。

IVrl: リボケーションリスト (Revocation List) のICV生成時に用いる初期値 (IV: Initial Value)。

IV_keys: メディア2で、コンテンツ暗号化用の鍵を暗号化する時の初期値 (IV: Initial Value)。

MKicv_bpt: アクセス許可情報であるBPT (Block Permission Table) のICV鍵を生成するマスター鍵。

IVicv_bpt: アクセス許可情報であるBPT (Block Permission Table) のICV鍵を生成する時のICV生成時に用いる初期値 (IV: Initial Value)。

IVbpt: アクセス許可情報であるBPT (Block Permission Table) の初期値 (IV: Initial Value)。

【0046】

・ECC回路323

送信レジスタ309、受信レジスタ310にあるデータについて、ECCチェックを行う専用ブロックである。

【0047】

・外部メモリ入出力インターフェイス324

外部メモリ (メディア1, 2) に対する入出力インターフェイス。外部メモリとしては例えばフラッシュメモリを搭載したメモリカード等がある。例えばコン

テンツ、およびコンテンツ記録再生に伴うヘッダ情報、さらにブロック・パーミッション・テーブル（BPT）がこの外部メモリ入出力インターフェイスを介して入出力する。

・内部メモリ入出力インターフェイス 325

内部メモリに対する入出力インターフェイス。当インタフェースを介して、内部メモリに格納された例えばリボケーションリストの入出力が実行される。

【0048】

外部メモリ入出力インターフェイス 324、および内部メモリ入出力インターフェイス 325からは、処理に応じて以下の各信号が外部メモリ（メディア1、2）、あるいは内部メモリに対して出力される。

CLE: コマンドラッチイネーブル

ALE: アドレスラッチイネーブル

CE: チップイネーブル

WE: ライトイネーブル

RE: リードイネーブル

また、外部メモリ（メディア1、2）、あるいは内部メモリからの信号として

WP: ライトプロテクト （外部メモリ（メディア1、2）にのみ適用）

RDY/BUSY: レディー・ビジー

これら各種信号が入力される。

【0049】

〔メモリ格納コンテンツ構成〕

次に、メディアのフラッシュメモリに格納されるコンテンツ構成について図6を用いて説明する。音楽データ、画像データ等、各コンテンツは、図6（a）に示すように各種属性情報からなるセキュリティヘッダと、実データ部としてのコンテンツとによって構成される。

【0050】

メディアのフラッシュメモリは、図6（b）に示すように、複数コンテンツのセキュリティヘッダ部とコンテンツ部との各ペアを格納する。前述したように、

フラッシュメモリはブロック単位で消去が実行されるので、1ブロックには同一コンテンツに関するセキュリティヘッダ部またはコンテンツ部を格納する形態とし、一括した消去処理が許容される場合を除いて、異なるコンテンツを1つのブロックに格納する処理は行なわない。

【0051】

[セキュリティヘッダ構成]

セキュリティヘッダは、各コンテンツに対応する属性情報である。セキュリティヘッダのデータ構成を図7に示す。各データ内容について説明する。

【0052】

・フォーマットバージョン (Format Version)

セキュリティヘッダ (Security Header) のフォーマットバージョンを示す。

・コンテンツID (Content ID)

コンテンツの識別子 (ID) を示す。

・コンテンツタイプ (Content Type)

コンテンツの種類を示す。例えばメディア1、またはメディア2に格納されたコンテンツ、あるいは放送コンテンツ等である。

・データタイプ (Data Type)

コンテンツの属性、例えば音楽、画像等のデータであるか、プログラムであるか等を示す。

・暗号アルゴリズム (Encryption Algorithm)

コンテンツのコンテンツ鍵 (Kc) を使った暗号化処理アルゴリズムを示す。例えばDESによる暗号化であるかトリプルDES (Triple-DES) によるか等を示す。

・暗号化モード (Encryption Mode)

暗号化アルゴリズム (Encryption Algorithm) で指定されたアルゴリズムに対応する暗号モードを示す。例えばECBモードかCBCモードか等を示す。

【0053】

・暗号化フォーマットタイプ (Encryption Format Type)

コンテンツの暗号化フォーマットを示す。タイプ1かタイプ2か、

コンテンツ全体に対して1つのコンテンツ鍵 K_c で暗号化するタイプをタイプ1とし、コンテンツのセクタ毎に異なる鍵 K_{sec_n} を適用してコンテンツの暗号化を行なう態様をタイプ2とする。

【0054】

図8に各タイプの暗号化フォーマット構成を示す。図8(a)がタイプ1の暗号化フォーマットで暗号化されたコンテンツのメモリ格納構成であり、(b)がタイプ2の暗号化フォーマットで暗号化されたコンテンツのメモリ格納構成である。

【0055】

図8(a)に示すタイプ1の暗号化フォーマットは、コンテンツがすべて1つのコンテンツ鍵 K_c を用いて暗号化されてメモリに格納された構成、すなわちセクタ非依存型暗号化処理である。図8(b)に示すタイプ2の暗号化フォーマットは、フラッシュメモリの各セクタ毎に異なるセクタ鍵 $K_{sec_1} \sim K_{sec_m}$ が適用されて暗号化されたコンテンツが格納された構成、すなわちセクタ依存型暗号化処理である。例えば図8(b)のフラッシュメモリのセクタ1では、セクタ1の暗号化鍵として K_{sec_1} が対応して設定され、セクタ1に格納されるコンテンツは、各ブロックにおいて、すべて K_{sec_1} を適用した暗号化処理が施されて格納される。フラッシュメモリのセクタmでは、セクタmの暗号化鍵として K_{sec_m} が対応して設定され、セクタmに格納されるコンテンツは、各ブロックにおいて、すべて K_{sec_m} を適用した暗号化処理が施されて格納される。

【0056】

このように、本発明の構成においては、各セクタ毎に異なる暗号化鍵を適用したコンテンツの暗号処理が適用される。さらに、各セクタ毎に異なる暗号化鍵を適用した処理態様においても、1つのセクタに1つの鍵を適用したシングルDESによる処理、1つのセクタに複数の鍵を適用したトリプルDESによる処理等、各種の暗号化態様が適用可能である。これらの処理形態については、さらに後段で詳細に説明する。

【0057】

図 7 に戻り、セキュリティヘッダの構成について説明を続ける。

・暗号化フラグ (Encryption Flag)

ブロック内の各セクタの暗号化・非暗号化を示すフラグ。ブロック内のセクタ数 (例えば 3 2 セクタ) 分のフラグを持つ。例えば 0 : 非暗号化セクタ、1 : 暗号化セクタ。なお、本例では 1 ブロックを 3 2 セクタとする。

【 0 0 5 8 】

・ I C V フラグ (ICV Flag)

ブロック内の各セクタの I C V 付加・非付加を示すフラグ。ブロック内のセクタ数 (32 セクタ) 分のフラグを持つ。例えば 0 : I C V なし、1 : I C V あり

【 0 0 5 9 】

・暗号化コンテンツ鍵 (K c _Encrypted 0-31)

暗号化されたコンテンツ鍵の格納領域 (32 個)

・暗号化 I C V 生成鍵 (K icv _cont _encrypted)

暗号化されたコンテンツの I C V 作成のための鍵の格納領域

【 0 0 6 0 】

・有効リボケーションリストバージョン (Valid Revocation List version)

コンテンツ再生の際に有効に適用されるリボケーションリスト (Revocation List) のバージョン。

コンテンツ再生の際に、セットされているリボケーションリスト (Revocation List) のバージョンがこれより古い場合、再生を許可しない。なお、自己デバイスにおいて格納したデータの再生処理等、リボケーションリストの参照を適用する必要がないコンテンツには 0 を設定する。

【 0 0 6 1 】

・セキュリティヘッダ I C V (ICV of Security Header)

セキュリティヘッダ (Security Header) の改竄チェック値 (I C V) 。

【 0 0 6 2 】

[リボケーションリスト]

次に、不正なメディアやコンテンツの失効情報としてのリボケーションリストの構成について説明する。図 9 にリボケーションリストの構成を示す。以下、各

データについて説明する。

【0063】

- ・リボケーションリスト識別子 (Revocation List ID)

リボケーションリスト (Revocation List) 固有の識別子としての ID である。

【0064】

- ・リボケーションリストバージョン (Revocation List Version)

リボケーションリスト (Revocation List) のバージョンを示す。リボケーションリストは、更新され、更新時に新たな不正なメディアやコンテンツの失効情報を追加する。

【0065】

本発明の構成では、リボケーションリスト (Revocation List) にバージョン情報を設定し、コンテンツのヘッダ内に有効なりボケーションリストのバージョン情報を設定する。コンテンツ読み出しの際に、現在デバイスに保持しているリボケーションリストのバージョンとコンテンツのヘッダ内にある有効なりボケーションリストのバージョンとを比較する。この際、現在保持しているリボケーションリストのバージョンの方がより古い場合には、コンテンツの読み出しを中止する。その結果、リボケーションリストの更新を行わなければ、そのコンテンツの読み出しはできない。

【0066】

また、リボケーションリストの更新時にメモリ・インターフェース部が現在のリボケーションリストのバージョン情報と更新用のリボケーションリストのバージョン情報とを比較して、新しいリボケーションリストであると判断した時のみ、リボケーションリスト更新を許可する構成とする。

【0067】

バージョン情報を用いたリボケーションリストの新旧比較処理、更新処理の具体的処理例については、処理フローを用いて後段で詳細に説明する。

【0068】

- ・メディア 1 ID 数 (Number of Media 1 ID)

失効しているメディア 1 (Media1 ID) の総数

・メディア 1 ID (0) - メディア 1 ID (L-1) (Media1ID(0) - Media1ID(L-1))

失効しているメディア 1 の識別子のリストである。

【0069】

・メディア 2 ID 数 (Number of Media2 ID)

失効しているメディア 2 (Media2 ID) の総数

・メディア 2 ID (0) - メディア 2 ID (M-1) (Media2ID(0) - Media2ID(M-1))

失効しているメディア 2 の識別子のリストである。

【0070】

・コンテンツ ID 数 (Number of Contents ID)

失効しているコンテンツ ID (Contents ID) の総数

・コンテンツ ID (0) - コンテンツ ID (N-1) (Contents ID(0) - Contents ID(N-1))

失効しているコンテンツ識別子のリストである。

【0071】

・リボケーションリスト IC V (ICV of Revocation List)

リボケーションリストの改竄チェック用の IC V

【0072】

上述のように、本発明におけるリボケーションリストは、複数の種類（メディア、コンテンツ）の識別子（ID）から構成される。このように、コンテンツやメディアの失効情報であるリボケーションリスト（Revocation List）に複数の種類のリボーク対象 ID、すなわちメディア ID、コンテンツ ID を設け、それぞれの照合を異なる動作として行うことによって、一つのリボケーションリストで複数のコンテンツ、メディアを排除することが可能となる。メディアの挿入時やコンテンツの読み出し時にメモリ・インターフェース部において、利用メディアまたは利用コンテンツの識別子（ID）と、リボケーションリストにリストされた ID との照合を実行することにより、不正なメディアの使用や不正なコンテ

ンツの読み出しを禁止することができる。

【0073】

このようにコンテンツやメディアの複数のIDを1つのリボケーションリストに設定した構成により1つのリボケーションリストで複数の種類のメディアとコンテンツのリボーク（排除）が可能になる。メディア起動時のリボケーションリストに基づくメディアの検証処理、コンテンツ処理時のコンテンツ検証処理の具体的処理については、後段で説明する。

【0074】

また、本発明の構成では、リボケーションリストは、外部メモリ等に直接アクセスするメモリインタフェースにセットアップされ、セットアップ後は、メディアの装着時、コンテンツの再生時においてメモリインタフェースにおいて継続的に利用可能な構成としたので、コンテンツの利用時に繰り返し内部メモリから読み出すなどの処理が不要となり処理が効率的に実行される。

【0075】

〔ブロック・パーミッション・テーブル（BPT）〕

次に、アクセス許可テーブルとして使用されるブロック・パーミッション・テーブル（BPT：Block Permission Table）の構成について説明する。従来、例えばPC等においてコンテンツの再生を実行する場合、PC内のOSのファイルシステムが主体的に、記録メディアに格納されているアクセス情報テーブル（例えば、File Allocation Table；FAT）を読み込んで管理しており、ファイルシステムがそのアクセス情報テーブルの内容を自由に書き換えが出来た。その為に、書き込み禁止を設定したアクセス情報テーブルを格納する記録メディアがあっても、そのアクセス情報テーブルをファイルシステムが読みとって書き換えることによって、記録メディア内のデータを書き換えられる可能性がある。

【0076】

本発明のデータ処理装置において採用されるブロック・パーミッション・テーブル（BPT）は、デバイスにおける書き替えを禁止したブロックに格納されるメディア自身のアクセス許可テーブルである。デバイスはBPTを格納したメディアを用いて、コンテンツデータ書き込み等のデータ処理を実行する場合、メデ

ィアに直接アクセスするデバイスのメモリアンターフェイス部にブロック・パーミッション・テーブル (BPT) をセットすることで、デバイスの制御部がいかなるプログラムを実行中でも、メディアのアクセス許可テーブルであるブロック・パーミッション・テーブル (BPT) に設定された許可情報に従ったメモリアクセスが行われる構成とした。

【0077】

図10にブロック・パーミッション・テーブル (BPT) の構成を示す。以下、各データについて説明する。

【0078】

・フォーマットバージョン (Format Version)

BPT (Block Permission Table) のフォーマットバージョンを示す。BPT 自体にも、各種のフォーマットがあり、そのいずれであるかを識別するデータである。

・BPT 識別子 (BPT ID)

ブロック・パーミッション・テーブル (BPT: Block Permission Table) の識別子 (ID) である。

・ブロック数 (Number of Blocks)

BPT (Block Permission Table) で扱うブロックの総数を示す。前述したように、フラッシュメモリはブロック毎の消去がなされる。BPTにより管理されるブロック数を示している。

・ブロック # 1 - ブロック # n 許可フラグ (Block #1 - #n Permission Flag)

各ブロックのアクセス制限フラグを示している。例えばフラグ0のブロックは、消去不可ブロックであり、フラグ1のブロックは消去可ブロックであることを示す。

・BPT-ICV (ICV of BPT)

BPT (Block Permission Table) の改竄チェック用のICVである。

【0079】

デバイスのファイルシステムはデバイスを認識した後に、ブロック・パーミッ

ション・テーブル（BPT）を例えばフラッシュメモリを搭載したメモリカード等のメディアから読み込み、メディアへ直接アクセスを行うメモリインターフェイス部にBPTを転送し、そのメディアに対するアクセス許可テーブルとして管理させる。メモリインターフェイス部は、アクセス許可テーブルを受信しBPTをセット（ex. 図4に示すメモリ部321）する。メモリインターフェイスは、メディアのメモリにアクセスする命令を受信した時、このメディアのアクセス許可テーブルに基づいたアクセスのみを実行する。

【0080】

ブロック・パーミッション・テーブル（BPT）には、例えばメディアのフラッシュメモリの各ブロック単位での許可された処理態様、具体的には例えば消去可ブロック、消去不可ブロック、あるいは再生可ブロック、再生不可ブロック等の設定がなされている。メモリインタフェースは、これらのBPT設定に従って処理の可否を決定する。これらの処理の詳細は、後段でさらに詳細に説明する。

【0081】

なお、ブロック・パーミッション・テーブル（BPT）には、改竄防止のための改竄チェック値ICVが設定され、BPTのメモリインタフェースへのセット時には、ICVチェックが実行され、改竄ありと判定された場合には、BPTのセット処理を実行しない。従って、不正なアクセス許可テーブルを作成して、使用することが防止される。BPTのICVはメディアの識別子（ID）に基づいて生成する。そのために、他のメディアにアクセス許可テーブルをコピーしたとしてもそのメディアは使用できない。ICVの生成については、後述する。

【0082】

メディアは、その製造時にブロック・パーミッション・テーブル（BPT）をメモリ（ex. フラッシュメモリ）の所定ブロックに書き込んで出荷する。この際、ブロック・パーミッション・テーブル（BPT）を格納したメモリ内のブロックについては、ブロック消去不可の設定をブロック・パーミッション・テーブル（BPT）に記述する。本発明のデバイスは、メディアに格納したデータ消去処理において、BPTを参照してBPTに設定された各ブロックの消去可否を参照した後、消去可であるブロックのみの消去を実行する構成であるので、BPT

格納ブロックを消去不可として設定したメディアについては、BPTの消去、書き換え替えが防止される。メディア内のBPTを利用したファイルの書き込み、再生処理については後述する。

【0083】

メディア（フラッシュメモリ搭載データ記録媒体）の製造時におけるブロック・パーミッション・テーブル（BPT）の設定フローを、図11および図12に示す。ここでは、メディアとコマンド通信が行えるメディア作成器を通してメディア識別子（ID）の生成とBPTの書き込みが連続動作で行われるものとする。

【0084】

図11は、相互認証処理機能を持たないメディア1のタイプにおけるメディア作成器が実行するブロック・パーミッション・テーブル（BPT）の設定フローである。各処理について説明する。まず、まだ初期設定が行われていないメディアに対し、ID読み出しコマンドを送って（S31）、あらかじめメディアに格納されたIDを受信（S32）すると、そのIDをベースとしたICV生成鍵 K_{icv_bpt} を生成（S33）する。ICV生成鍵 K_{icv_bpt} は、マスター鍵： MK_{icv_bpt} と、初期値： IV_{icv_bpt} と、BPT識別子（ID）に基づいて生成する。具体的には、 $ICV生成鍵 K_{icv_bpt} = DES(E, MK_{icv_bpt}, ID \oplus IV_{icv_bpt})$ に基づいて生成される。式の意味は、BPTのIDと初期値 IV_{icv_bpt} の排他論理和にマスター鍵： MK_{icv_bpt} によるDESモードでの暗号化処理を実行するという意味である。

【0085】

次に、BPTの各フィールドに必要なパラメータを設定（S34）し、各パラメータが設定されたBPTに基づいてICVを生成（後述する図14の構成を適用）し（S35）、生成したICVをBPTのICVフィールドに設定（S36）する。このようにして構成されたブロック・パーミッション・テーブル（BPT）をメディア1に書き込む（S37）。なお、前述したようにBPTの書き込みブロックは、BPTにおいて消去不可領域として設定されたブロックとする。

【0086】

図 1 2 は、相互認証処理機能を持つメディア 2 のタイプにおけるメディア作成器が実行するブロック・パーミッション・テーブル (BPT) の設定フローである。各処理について説明する。まず、まだ初期設定が行われていないメディア 2 との相互認証処理およびセッション鍵の共有 (これらの処理については、後述する図 2 2 の処理を参照) を実行する。

【0087】

相互認証および鍵共有処理が終了すると、メディア 2 に対し ID 読み出しコマンドを送って (S 4 1)、ID を読み出し、ID をベースとした ICV 生成鍵 K_{icv_bpt} を生成 (S 4 2) する。ICV 生成鍵 K_{icv_bpt} は、マスター鍵: MK_{icv_bpt} と、初期値: IV_{icv_bpt} と、BPT 識別子 (ID) に基づいて生成する。具体的には、 $ICV \text{ 生成鍵 } K_{icv_bpt} = DES(E, MK_{icv_bpt}, ID \oplus IV_{icv_bpt})$ に基づいて生成される。式の意味は、BPT の ID と初期値 (IV_{icv_bpt}) の排他論理和にマスター鍵: MK_{icv_bpt} による DES モードでの暗号化処理を実行するという意味である。

【0088】

次に、BPT の各フィールドに必要なパラメータを設定 (S 4 5) し、各パラメータが設定された BPT に基づいて ICV を生成 (後述する図 1 4 の構成を適用) し (S 4 6)、生成した ICV を BPT の ICV フィールドに設定 (S 4 7) する。このようにして構成されたブロック・パーミッション・テーブル (BPT) をメディア 1 に書き込む (S 4 8)。なお、前述したように BPT の書き込みブロックは、BPT において消去不可領域として設定されたブロックとする。

【0089】

図 1 3 にブロック・パーミッション・テーブル (BPT) の具体的構成例を示す。図 1 3 の (a) はメディア 1、メディア 2 のフラッシュメモリのブロック構成であり、図 1 3 (b) は、ブロック・パーミッション・テーブル (BPT) である。ブロック・パーミッション・テーブル (BPT) は、フォーマット・バージョン、BPT ID、ブロック数に続いて、各ブロックの消去可 (1)、消去不可 (0) が設定され、最後に BPT の改竄チェック値 (ICV of BPT) が格納された構成を持つ。メモリの BPT 格納ブロック (図 1 3 の例ではブロック

2) は、ブロック・パーミッション・テーブル (BPT) において消去不可領域として設定され、デバイスによる消去を防止し、BPTの書き替えが実行されない構成を持つ。

【0090】

なお、図13に示すブロック・パーミッション・テーブル (BPT) の構成例は、各ブロックの消去可 (1)、消去不可 (0) のみが設定された構成であるが、消去処理のみのアクセス許可を設定する構成ではなく、読み取り (再生) 許可、不許可を設定した構成としてもよい。例えば再生および消去不可 (11)、再生可、消去不可 (10)、再生不可、消去可 (01)、再生および消去可 (00) とした設定が可能である。

【0091】

なお、図2に示したようにメディア2ではメディア内に制御部231を持っており、ブロック・パーミッション・テーブル (BPT) が設定済みかどうかの状態を保持することもでき、BPTが設定されている状態で、デバイスからBPTの新たな書き込み命令が来たとしても、受け付けない構成として、BPTの再書き込みを防止する構成としてもよい。

【0092】

なお、上述の例におけるBPT書き込みは、メディアとコマンド通信が行えるメディア作成器を通して実行する構成について説明したが、この他、メディアへのBPTの書き込みは、単純なメモリライターで作成したBPTを直接書き込む構成としてもよい。ただし、この場合も、メモリのBPT格納ブロックは、ブロック・パーミッション・テーブル (BPT) において消去不可領域として設定する。

【0093】

[改竄チェック値 (ICV) による改竄チェック]

次に、改竄チェック値 (ICV: Integrity Check Value) によるデータ改竄チェック処理について説明する。本発明の構成において、改竄チェック値 (ICV) は、データ記憶手段に格納されるコンテンツ、ブロック・パーミッション・テーブル、リボケーションリスト等に付加され、それぞれのデータ改竄チェック

処理に適用される。なお、コンテンツについての改竄チェック値は、セクタデータ単位に付加可能な構成である。コンテンツ、ブロック・パーミッション・テーブル、リボケーションリスト等に付加されたICV処理の具体的形態については、後段で説明する。

【0094】

DES暗号処理構成を用いた改竄チェック値(ICV)生成例を図14に示す。図14の構成に示すように対象となる改竄チェックデータを構成するメッセージを8バイト単位に分割(以下、分割されたメッセージをD0、D1、D2、・・・、Dn-1とする)する。改竄チェックデータは、例えばコンテンツ自体であったり、上述したアクセス許可テーブルであるBPTの構成データであったり、あるいはリボケーションリストの構成データである。

【0095】

まず、初期値(Initial Value (以下、IVとする))とD0を排他的論理和する(その結果をI1とする)。次に、I1をDES暗号化部に入れ、改竄チェック値(ICV)生成鍵K_{icv}を用いて暗号化する(出力をE1とする)。続けて、E1およびD1を排他的論理和し、その出力I2をDES暗号化部へ入れ、改竄チェック値(ICV)生成鍵K_{icv}を用いて暗号化する(出力E2)。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたENをコンテンツチェック値ICV'とする。

【0096】

改竄のないことが保証された例えばコンテンツ生成時に生成した正当なICVと、新たにコンテンツに基づいて生成したICV'とを比較して同一性が立証、すなわちICV' = ICVであれば入力メッセージ、例えばコンテンツ、BPT、あるいはリボケーションリストに改竄のないことが保証され、ICV' ≠ ICVであれば改竄があったと判定される。

【0097】

ICVを使用したデータ改竄チェック処理フローを図15に示す。まず、改竄チェックの対象データを抽出し(S11)、抽出したデータに基づいて例えば図14のDES暗号処理構成によりICV'を計算する(S12)。計算の結果、

算出された I C V' とデータ内に格納された I C V とを比較し (S 1 3)、一致した場合は、データの改竄が無く正当なデータであると判定 (S 1 4 から S 1 5) され、不一致の場合は、データの改竄があると判定 (S 1 4 から S 1 6) される。

【0098】

リボケーションリストの改竄チェック用の改竄チェック値 (I C V) 生成鍵 K_{icv_rl} は、予めデバイスのメモリインタフェース部 300 のメモリ部 321 (図 4 参照) 内に格納されたりボケーションリスト (Revocation List) の I C V 鍵を生成するマスター鍵: MK_{icv_rl} と、リボケーションリスト (Revocation List) の I C V 鍵を生成する時の初期値: IV_{icv_rl} と、リボケーションリストの属性情報中に含まれるリボケーションリスト・バージョン (Version) に基づいて生成する。具体的には、改竄チェック値 (I C V) 生成鍵 $K_{icv_rl} = DES(E, MK_{icv_rl}, Version \oplus IV_{icv_rl})$ に基づいて生成される。前記式の意味は、バージョン (Version) と初期値 (IV_{icv_rl}) の排他論理和にマスター鍵: MK_{icv_rl} による DES モードでの暗号化処理を実行するという意味である。リボケーションリストの改竄チェック値は、このようにして生成された I C V 生成鍵 K_{icv_rl} を適用して初期値 IV_{rl} (メモリ部 321 に格納) を用いて図 15 に示す I C V 生成構成によって実行される。

【0099】

また、ブロック・パーミッション・テーブル (BPT) の改竄チェック用の改竄チェック値 (I C V) 生成鍵 K_{icv_bpt} は、予めデバイスのメモリインタフェース部 300 のメモリ部 321 (図 4 参照) 内に格納された BPT の I C V 鍵を生成するマスター鍵: MK_{icv_bpt} と、BPT の I C V 鍵を生成する時の初期値: IV_{icv_bpt} と、BPT の属性情報中に含まれる BPT 識別子 (ID) に基づいて生成する。具体的には、改竄チェック値 (I C V) 生成鍵 $K_{icv_bpt} = DES(E, MK_{icv_bpt}, ID \oplus IV_{icv_bpt})$ に基づいて生成される。前記式の意味は、BPT の ID と初期値 (IV_{icv_bpt}) の排他論理和にマスター鍵: MK_{icv_bpt} による DES モードでの暗号化処理を実行するという意味である。ブロック・パーミッション・テーブル (BPT) の改竄チェック値は、

このようにして生成されたICV生成鍵 K_{icv_bpt} を適用して初期値 IV_{bpt} （メモリ部321に格納）を用いて図15に示すICV生成構成によって実行される。なお、BPTの付帯情報として格納されるICVは、BPT内のデータとBPTを格納したメディアの識別子（ID）を含むデータに基づいて生成される。従って、BPTのICVチェックは、BPTのデータ改竄の有無のみならず、メディア固有の正当なBPT、すなわち他のメディアにコピーされたBPTでないことを検証する機能も兼ね備える。

【0100】

また、コンテンツのセクタ単位の改竄チェック用の改竄チェック値（ICV）生成鍵 K_{icv_cont} は、コンテンツのヘッダ（セキュリティ・ヘッダ）中に暗号化されて格納されており、必要に応じてメモリインタフェースの暗号処理部320（図4参照）において、また、メディア2との相互認証後に実行されるメディア2のコントローラ231で実行されるDES-CBCモードによる復号処理によって取得される。これらの処理についてはフローを用いた説明中で詳細に説明する。

【0101】

このようなデータ改竄チェックの結果、例えばリボケーションリストの改竄が明らかになれば、リボケーションリストの参照処理に基づくコンテンツの再生等の処理を禁止し、また、アクセス許可テーブルであるBPTに改竄があると判定されれば、BPTに基づくメディアのデータに対するアクセスを禁止する処理を実行する。これらの処理については、後段で詳細に説明する。

【0102】

【データ読み出し、書き込み処理】

以下、本発明のデータ処理装置において、デバイスがメディアからのデータ読み出しを行なう場合の処理、およびデバイスがメディアに対してデータを格納する場合に実行される処理について説明する。

【0103】

（デバイス起動時処理）

まず、デバイスを起動させた場合における処理を図16を用いて説明する。図

16は、左側に図2におけるデバイス200の制御部205の処理、右側にメモリーインタフェース部300の処理を示したものである。処理スタート時点でのメモリーインタフェース部300のステータスレジスタの状態は、ビジーフラグ：0（待機）、リボケーションリストセットフラグ：0（未セット）である。

【0104】

まず、デバイスが起動すると、制御部は、内部メモリのファイル割り当てテーブル呼び出しコマンドをメモリーインタフェース部に送信（S101）する。メモリーインタフェース部は、デバイスの内部メモリに対してファイル割り当てテーブルの読み出しコマンドを送信（S102）して、ファイル割り当てテーブルを内部メモリから受信し、制御部に送信（S103）する。

【0105】

なお、ファイル割り当てテーブルは、デバイスのアクセス可能な内部メモリ、外部メモリに格納されたデータ、例えば様々なコンテンツ、あるいはリボケーションリスト等、各種データファイルをディレクトリ管理するテーブルであり、例えば図17に示すように、ディレクトリ、ファイル名、格納セクタが対応付けられた構成を持つ。デバイスは、ファイル割り当てテーブルに基づいて、様々なファイルのアクセスを行なう。

【0106】

制御部は、内部メモリに格納されたデータに対応するファイル割り当てテーブルを受信（S104）すると、テーブルに基づいてリボケーションリストの読み出し処理を実行（S105）し、リボケーションリストのセットコマンドと、リボケーションリストをメモリーインタフェース部に送信（S106）する。リボケーションリストのセット処理は、リボケーションリストが有効である場合にのみ実行され、リストがセットされると、メディアからのコンテンツ読み出し処理等、コンテンツ処理の際、リボケーションリストにリストアップされたコンテンツまたはメディア識別子との比較処理を実行する。これらの処理については後述する。

【0107】

リボケーションリストのセットコマンドと、リボケーションリストを制御部か

ら受信 (S107) すると、メモリアンタフェースは、ステータスレジスタのビジーフラグを1 (ビジー) にセット (S108) し、リボケーションリストの改竄チェック用の改竄チェック値 (ICV) 生成鍵 K_{icv_rl} を生成 (S109) する。

【0108】

リボケーションリストの改竄チェック用の改竄チェック値 (ICV) 生成鍵 K_{icv_rl} は、予めデバイス内に格納されたリボケーションリスト (Revocation List) の ICV 鍵を生成するマスター鍵: MK_{icv_rl} と、リボケーションリスト (Revocation List) の ICV 鍵を生成する時の初期値: IV_{icv_rl} と、リボケーションリストの属性情報中に含まれるリボケーションリスト・バージョン (Version) に基づいて生成する。具体的には、改竄チェック値 (ICV) 生成鍵 $K_{icv_rl} = DES(E, MK_{icv_rl}, Version \oplus IV_{icv_rl})$ に基づいて生成される。式の意味は、バージョン (Version) と初期値 (IV_{icv_rl}) の排他論理和にマスター鍵: MK_{icv_rl} による DES モードでの暗号化処理を実行するという意味である。

【0109】

次にメモリアンタフェースは生成した改竄チェック値 (ICV) 生成鍵 K_{icv_rl} を用いてリボケーションリストの ICV' を生成し、予めリボケーションリスト内に格納された正しい ICV との照合処理 ($ICV' = ICV?$) を実行 (S110) する。なお、 ICV' の生成処理は、前述の図14で説明した DES モードに基づいて、初期値 IV_{rl} を用い、生成した改竄チェック値 (ICV) 生成鍵 K_{icv_rl} を適用した処理によって行われる。

【0110】

$ICV' = ICV$ である場合 (S111で Yes) は、リボケーションリストが改竄のない正当なものであると判定され、コンテンツの読み出し処理等の際に参照可能な状態にセットし、リボケーションリストセットフラグを1 (セット) にセット (S112) する。リボケーションリストはメモリアンタフェース内のメモリ (例えばメモリ部321 (図4参照)) に格納され、例えば、送受信制御部306が制御部205 (図2参照) からメディア認識コマンドを受信するとセ

ットされたりボケーションリストのメディア識別子と、デバイスに装着したメディアのメディア識別子との照合が実行され、また、送受信制御部 3 0 6 が制御部 2 0 5 からコンテンツの読み出し処理に伴うヘッダセットコマンドを受信するとセットされたりボケーションリストのコンテンツ識別子と、読み出し対象コンテンツのコンテンツ識別子との照合が実行される。

【0 1 1 1】

このように、リボケーションリストは、外部メモリ等に直接アクセスするメモリインタフェースにセットアップされ、セットアップ後は、メディアの装着時、コンテンツの再生時においてメモリインタフェースにおいて継続的に利用可能な構成とされ、コンテンツの利用時に繰り返し内部メモリから読み出すなどの処理が不要となり処理が効率的に実行される。

【0 1 1 2】

図 1 6 のフローの説明を続ける。ICV' ≠ ICV である場合 (S 1 1 1 で N o) は、リボケーションリストに改竄ありと判定され、リストの参照処理に基づくコンテンツ処理を禁止し処理を終了する。以上の処理の終了により、ビジーフラグは 0 にセットされる。

【0 1 1 3】

一方、制御部側は、ステータス読み出しコマンドをメモリインタフェースに送信 (S 1 1 4) し、ビジーフラグが 0 となったことを条件 (S 1 1 5) としてリボケーションリストセットフラグを保存 (S 1 1 6) する。保存されるリボケーションセットフラグは、リストの改竄が無いと判定された場合は、リストが有効にセットされたことを示す 1、その他の場合は 0 となる。

【0 1 1 4】

(メディア認識時処理)

次に、デバイスにメディアが装着された場合のメディアの有効性確認等、メディア認識時に実行する処理について説明する。前述したようにメディアには、デバイスとの相互認証処理を実行しないタイプのメディア 1 と、デバイスとの相互認証処理を実行するタイプのメディア 2 とがある。デバイスは、それぞれのタイプがデバイスに装着されると、メディアを利用したコンテンツ処理を実行してよ

いか否か、具体的にはリボケーションリストに不正メディアとしての登録がないかを確認する処理を実行し、装着メディアがリボケーションリストにリストアップされておらず、有効に利用可能なメディアであることが確認されたことを条件として、メディアに格納されたアクセス許可テーブルであるBPT (Block Permission Table) をメモリインタフェースにセットし、BPTを参照したメモリアクセスを可能とする処理を実行する。

【0115】

まず、メディア1が装着された場合のメディア確認処理について図18、図19を用いて説明する。

【0116】

図18、図19においても左側に図2におけるデバイス200の制御部205の処理、右側にメモリインタフェース部300の処理を示している。当フロー開始時点で、メモリインタフェース部300のステータスレジスタの状態は、ビジーフラグ：0（待機）、メディア1有効フラグ：0（無効）、メディア1セットフラグ：0（未セット）の状態である。

【0117】

まず、制御部は、デバイスに装着されたメディアがメディア1であることを認識する（S201）。メディア識別は予め設定されたメディア形状に基づく機械的情報あるいはデバイス、メディア間の通信情報に基づいて行われる。制御部がメディア1であることを認識すると制御部は、メディア1認識コマンドをメモリインタフェースに送信する（S202）。

【0118】

メモリインタフェースは、制御部からのメディア1認識コマンドを受信（S203）すると、ステータスレジスタのビジーフラグを1（ビジー）に設定し（S204）、メディア1に対してメディア1の識別子（ID）の読み出しコマンドを送信（S205）し、受信（S206）する。さらに、受信したメディア1のIDと、既にセットされているリボケーションリスト中のリボーク（排除）メディア1のリストとの比較照合を実行（S207）する。リボケーションリストは、先の図16の起動時フローにおいて説明したように、起動時にメモリインタフ

ェースにセットアップされ、セットアップ後は、メディアの装着時、コンテンツの再生時においてメモリインタフェースにおいて継続的に利用可能となる。

【0119】

受信IDと一致するIDがリスト中に存在しなかった場合は、装着メディア1はリボーク対象メディアではなく、有効に利用可能なメディアであると判定（S208においてNo）し、ステータスレジスタのメディア1有効フラグを1（有効）にセット（S209）し、ビジーフラグを0（待機）にセット（S210）する。受信IDと一致するIDがリボケーションリスト中にあった場合（S208においてYes）は、装着メディア1はリボーク対象メディアであり、有効に利用できないと判定し、ステップS209の有効フラグの有効化処理を実行せずステップS210でビジーフラグを0（待機）にセットして処理を終了する。

【0120】

一方、制御部は、ステップS211において、ステータス読み出しコマンドをメモリインタフェースに送信し、ビジーフラグが0（待機）になったことを確認（S212）の後、メディアフラグ状態を確認して有効（フラグ：1）である場合（S213でYes）にのみ処理を続行し、無効（フラグ：0）である場合（S213でNo）は、処理を終了する。

【0121】

次に、図19に進み、制御部は、メディア1に関するファイル割り当てテーブル呼び出しコマンドをメモリインタフェースに送信（S221）し、メモリインタフェースは、ファイル割り当てテーブルの格納されたセクタ読み出しコマンドをメディア1に送信（S222）し、ファイル割り当てテーブルをメディア1から受信し、制御部に送信（S223）する。

【0122】

制御部は、メディア1に格納されたデータに対応するファイル割り当てテーブルを受信（S224）すると、テーブルに基づいてブロック・パーミッション・テーブル（BPT）の読み出し処理を実行（S225）し、BPTのセットコマンドと、BPTをメモリインタフェースに送信（S226）する。BPTのセット処理は、BPTが有効である場合にのみ実行され、BPTがセットされると、

メディアからのコンテンツ書き込み処理等、コンテンツ処理の際、BPTを参照してブロック毎の消去が可能か否かを判定する。実際のBPTを参照したデータ書き込み処理については、後段で説明する。

【0123】

ブロック・パーミッション・テーブル(BPT)のセットコマンドと、BPTを制御部から受信(S227)すると、メモリインタフェースは、ステータスレジスタのビジーフラグを1(ビジー)にセット(S228)し、BPTの改竄チェック用の改竄チェック値(ICV)生成鍵 K_{icv_bpt} を生成(S229)する。

【0124】

BPTの改竄チェック用の改竄チェック値(ICV)生成鍵 K_{icv_bpt} は、予めデバイス内に格納されたBPTのICV鍵を生成するマスター鍵： MK_{icv_bpt} と、BPTのICV鍵を生成する時の初期値： IV_{icv_bpt} と、メディアIDに基づいて生成する。具体的には、改竄チェック値(ICV)生成鍵 $K_{icv_bpt} = DES(E, MK_{icv_bpt}, \text{メディアID} \wedge IV_{icv_bpt})$ に基づいて生成される。式の意味は、メディアIDと初期値(IV_{icv_bpt})の排他論理和にマスター鍵： MK_{icv_bpt} によるDESモードでの暗号化処理を実行するという意味である。

【0125】

次にメモリインタフェースは生成した改竄チェック値(ICV)生成鍵 K_{icv_bpt} を用いてBPTの ICV' を生成し、予めBPT内に格納された正しいICV値との照合処理($ICV' = ICV?$)を実行(S230)する。なお、 ICV' の生成処理は、前述の図14で説明したDESモードに基づいて、初期値 IV_{bpt} を用い、生成した改竄チェック値(ICV)生成鍵 K_{icv_bpt} を適用した処理によって行われる。なお、BPTの付帯情報として格納されたICVは、メディアIDを含むデータに基づいて生成されており、ICVのチェックは、BPTのデータ改竄の有無のみならず、メディア固有の正当なBPT、すなわち他のメディアにコピーされたBPTでないことの検証も兼ね備える機能を持つ。

【0126】

ICV' = ICVである場合 (S 2 3 1でYes) は、BPTが正当なメディアに格納された改竄のない正当なものであると判定され、コンテンツ処理等の際に参照可能な状態にセットし、メディア1セットフラグを1 (セット) にセット (S 2 3 2) する。ICV' ≠ ICVである場合 (S 2 3 1でNo) は、BPTに改竄ありと判定され、BPTの参照処理に基づくコンテンツ処理を禁止し処理を終了する。以上の処理の終了により、ビジーフラグは0にセット (S 2 3 3) される。

【0 1 2 7】

一方、制御部側は、ステータス読み出しコマンドをメモリインタフェースに送信 (S 2 3 4) し、ビジーフラグが0となったことを条件 (S 2 3 5でYes) としてメディア1セットフラグを保存 (S 2 3 6) する。保存されるメディア1セットフラグは、BPTの改竄が無いと判定された場合は、メディア1が有効にセットされたことを示す1、その他の場合は0となる。

【0 1 2 8】

次にメディア2がデバイスに装着された際のメディア2確認処理について、図20、図21を用いて説明する。メディア2は、図2を用いて説明したように、デバイスとの相互認証を実行するメディアである。

【0 1 2 9】

図20のステップS 3 0 1からS 3 0 4のステップは、メディア1の確認処理におけるステップS 2 0 1～S 2 0 4と同様であるので説明を省略する。

【0 1 3 0】

ステップS 3 0 5において、メモリインタフェースは、メディア2との相互認証処理を実行する。

【0 1 3 1】

図22に、共通鍵暗号方式を用いた相互認証方法 (ISO/IEC 9798-2) の処理シーケンスを示す。図22においては、共通鍵暗号方式としてDESを用いているが、共通鍵暗号方式であれば他の方式も可能である。図22において、まず、Bが64ビットの乱数Rbを生成し、Rbおよび自己のIDであるID(b)をAに送信する。これを受信したAは、新たに64ビットの乱数Raを生成し、Ra

、 R_b 、 $ID(b)$ の順に、DESのCBCモードで鍵 K_{ab} を用いてデータを暗号化し、 B に返送する。なお、鍵 K_{ab} は、 A および B に共通の秘密鍵、認証鍵である。DESのCBCモードを用いた鍵 K_{ab} による暗号化処理は、例えばDESを用いた処理においては、初期値と R_a とを排他的論理和し、DES暗号化部において、鍵 K_{ab} を用いて暗号化し、暗号文 E_1 を生成し、続けて暗号文 E_1 と R_b とを排他的論理和し、DES暗号化部において、鍵 K_{ab} を用いて暗号化し、暗号文 E_2 を生成し、さらに、暗号文 E_2 と $ID(b)$ とを排他的論理和し、DES暗号化部において、鍵 K_{ab} を用いて暗号化して生成した暗号文 E_3 とによって送信データ(Token-AB)を生成する。

【0132】

これを受信した B は、受信データを、やはり共通の秘密鍵としてそれぞれの記録素子内に格納する鍵 K_{ab} (認証鍵)で復号化する。受信データの復号化方法は、まず、暗号文 E_1 を認証鍵 K_{ab} で復号化し、初期値と排他的論理和し乱数 R_a を得る。次に、暗号文 E_2 を認証鍵 K_{ab} で復号化し、その結果と E_1 を排他的論理和し、 R_b を得る。最後に、暗号文 E_3 を認証キー K_{ab} で復号化し、その結果と E_2 を排他的論理和し、 $ID(b)$ を得る。こうして得られた R_a 、 R_b 、 $ID(b)$ のうち、 R_b および $ID(b)$ が、 B が送信したものと一致するか検証する。この検証に通った場合、 B は A を正当なものとして認証する。

【0133】

次に B は、認証後に使用するセッションキー(K_{ses})を乱数によって生成する。そして、 R_b 、 R_a 、 K_{ses} の順に、DESのCBCモードで認証キー K_{ab} を用いて暗号化し、 A に返送する。

【0134】

これを受信した A は、受信データを認証キー K_{ake} で復号化する。受信データの復号化方法は、 B の復号化処理と同様である。こうして得られた R_b 、 R_a 、 K_{ses} の内、 R_b および R_a が、 A が送信したものと一致するか検証する。この検証に通った場合、 A は B を正当なものとして認証する。互いに相手を認証した後は、セッションキー K_{ses} は、認証後の秘密通信のための共通鍵として利用される。

【0135】

なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものと、その後の相互間のデータ通信処理が禁止される。

【0136】

図23、図24に本発明のデバイスとメディア間における相互認証、鍵（セッション鍵）共有処理フローを示す。図23、図24において、左側がデバイスのメモリインタフェース、右側がメディア2のコントローラにおける処理である。

【0137】

まず、メディア2コントローラが乱数 R_a を生成（S401）し、 R_a および自己のIDであるメディア2IDをデバイスメモリインタフェースに送信（S402）する。これを受信（S403）したデバイスメモリインタフェースは、受信したメディア2IDと、初期値（ IV_ake ）の排他論理和に自己の所有する認証鍵生成用マスター鍵： MK_ake を適用しDES暗号化処理を行なって認証鍵 K_ake を生成（S404）する。さらに、デバイスメモリインタフェースは、新たに乱数 R_b を生成（S405）し、初期値 IV_auth と R_b とを排他的論理和し、鍵 K_ake を用いて暗号化し、暗号文 E_1 を生成し、続けて暗号文 E_1 と R_a とを排他的論理和し、鍵 K_ake を用いて暗号化して暗号文 E_2 を生成し、さらに、暗号文 E_2 とメディア2IDとを排他的論理和し、鍵 K_ake を用いて暗号化して暗号文 E_3 を生成し（S406）、生成したデータ $E_1||E_2||E_3$ をメディア2コントローラに送信（S407）する。[||]は、データの結合を意味する。

【0138】

これを受信（S408）したメディア2コントローラは、受信データを、認証鍵 K_ake で復号化（S409）する。受信データの復号化方法は、まず、暗号文 E_1 を認証鍵 K_ake で復号化し、初期値と排他的論理和し乱数 R_b' を得る。次に、暗号文 E_2 を認証鍵 K_ake で復号し、その結果と E_1 を排他的論理和し、 R_a' を得る。最後に、暗号文 E_3 を認証鍵 K_ake で復号し、その結果と E_2 を排他的論理和し、メディア2ID'を得る。こうして得られた R_a' 、 R_b' 、メディア2ID'のうち、 R_a' およびメディア2ID'が、メディア2

が送信したものと一致するか検証 (S410, S411) する。この検証に通った場合、メディア2はデバイスを正当なものとして認証する。Ra' およびメディア2 ID' が、送信データと不一致であったときは、相互認証が失敗 (S413) したものとし、その後のデータ通信を中止する。

【0139】

次にメディア2コントローラは、認証後に使用するセッションキー (Kses) としての乱数を生成 (S412) する。次に、図24のステップS421において、Ra、Rb、Ksesの順に、DESのCBCモードで認証鍵Kakeを用いて暗号化し、デバイスメモリインタフェースに送信 (S422) する。

【0140】

これを受信 (S423) したデバイスメモリインタフェースは、受信データを認証鍵Kakeで復号 (S424) する。こうして得られたRa"、Rb"、Ksesの内、Ra" およびRb" が、デバイスが送信したものと一致するか検証 (S425, S426) する。この検証に通った場合、デバイスはメディア2を正当なものとして認証 (S427) する。互いに相手を認証した後は、セッションキーKsesを共有 (S429) し、認証後の秘密通信のための共通鍵として利用される。Ra" およびRb" が、送信データと不一致であったときは、相互認証が失敗 (S428) したものとし、その後のデータ通信を中止する。

【0141】

図20に戻り、メディア2の認識処理について説明を続ける。ステップS305において上述の相互認証、鍵共有処理が実行され、ステップS306で相互認証が成功したことが確認されると、相互認証処理時に受信したメディア2のIDと、既にセットされているリボケーションリスト中のリボーク (排除) メディア2のリストとの比較照合を実行 (S307) する。

【0142】

受信IDと一致するIDがリスト中に存在しなかった場合は、装着メディア2はリボーク対象メディアではなく、有効に利用可能なメディアであると判定 (S308においてNo) し、ステータスレジスタのメディア2有効フラグを1 (有効) にセット (S309) し、ビジーフラグを0 (待機) にセット (S310)

する。受信IDと一致するIDがリボケーションリスト中にあった場合（S308においてYes）は、装着メディア2はリボーク対象メディアであり、有効に利用できないと判定し、ステップS309の有効フラグの有効化処理を実行せずステップS310でビジーフラグを0（待機）にセットして処理を終了する。

【0143】

一方、制御部は、ステップS311において、ステータス読み出しコマンドをメモリインタフェースに送信し、ビジーフラグが0（待機）になったことを確認（S312）の後、メディアフラグ状態を確認して有効（フラグ：1）である場合（S313でYes）にのみ処理を続行し、無効（フラグ：0）である場合（S313でNo）は、処理を終了する。

【0144】

次に、図21に進み、制御部は、メディア2に関するファイル割り当てテーブル呼び出しコマンドをメモリインタフェースに送信（S321）し、メモリインタフェースは、ファイル割り当てテーブルの格納されたセクタ読み出しコマンドをメディア2に送信（S322）し、ファイル割り当てテーブルをメディア2から受信し、制御部に送信（S323）する。

【0145】

制御部は、メディア2に格納されたデータに対応するファイル割り当てテーブルを受信（S324）すると、テーブルに基づいてブロック・パーミッション・テーブル（BPT）の読み出し処理を実行（S325）し、BPTのセットコマンドと、BPTをメモリインタフェースに送信（S326）する。BPTのセット処理は、BPTが有効である場合にのみ実行され、BPTがセットされると、メディアからのコンテンツ書き込み処理等、コンテンツ処理の際、BPTを参照してブロック毎の消去が可能か否かを判定する。実際のBPTを参照したデータ書き込み処理については、後段で説明する。

【0146】

ブロック・パーミッション・テーブル（BPT）のセットコマンドと、BPTを制御部から受信（S327）すると、メモリインタフェースは、ステータスレジスタのビジーフラグを1（ビジー）にセット（S328）し、BPTの改竄チ

エック用の改竄チェック値 (ICV) 生成鍵 K_{icv_bpt} を生成 (S329) する。

【0147】

BPTの改竄チェック用の改竄チェック値 (ICV) 生成鍵 K_{icv_bpt} は、予めデバイス内に格納されたBPTのICV鍵を生成するマスター鍵： MK_{icv_bpt} と、BPTのICV鍵を生成する時の初期値： IV_{icv_bpt} と、メディア2IDに基づいて生成する。具体的には、改竄チェック値 (ICV) 生成鍵 $K_{icv_bpt} = DES(E, MK_{icv_bpt}, \text{メディア2ID} \cdot IV_{icv_bpt})$ に基づいて生成される。式の意味は、メディア2IDと初期値 (IV_{icv_bpt}) の排他論理和にマスター鍵： MK_{icv_bpt} によるDESモードでの暗号化処理を実行するという意味である。

【0148】

次にメモリインタフェースは生成した改竄チェック値 (ICV) 生成鍵 K_{icv_bpt} と IV_{bpt} を用いてBPTのICV' を生成し、予めBPT内に格納された正しいICV値との照合処理 ($ICV' = ICV?$) を実行 (S330) する。なお、ICV' の生成処理は、前述の図14で説明したDESモードに基づいて、初期値 IV_{bpt} を用い、生成した改竄チェック値 (ICV) 生成鍵 K_{icv_bpt} を適用した処理によって行われる。なお、BPTの付帯情報として格納されたICVは、メディア2IDを含むデータに基づいて生成されており、ICVのチェックは、BPTのデータ改竄の有無のみならず、メディア固有の正当なBPT、すなわち他のメディアにコピーされたBPTでないことの検証も兼ね備える機能を持つ。

【0149】

$ICV' = ICV$ である場合 (S331でYes) は、BPTが正当なメディアに格納された改竄のない正当なものであると判定され、コンテンツ処理等の際に参照可能な状態にセットし、メディア2セットフラグを1 (セット) にセット (S332) する。 $ICV' \neq ICV$ である場合 (S331でNo) は、BPTに改竄ありと判定され、BPTの参照処理に基づくコンテンツ処理を禁止し処理を終了する。以上の処理の終了により、ビジーフラグは0にセット (S333)

される。

【0150】

一方、制御部側は、ステータス読み出しコマンドをメモリインタフェースに送信（S334）し、ビジーフラグが0となったことを条件（S335でYes）としてメディア2セットフラグを保存（S336）する。保存されるメディア2セットフラグは、BPTの改竄が無いと判定された場合は、メディア2が有効にセットされたことを示す1、その他の場合は0となる。

【0151】

（データファイル読み出し処理）

次に、データファイルの読み出し処理について図25のフローを用いて説明する。データファイルには、音楽データ、画像データ等のコンテンツデータファイル、さらに前述したリボケーションリストも含まれる。図25に示すフローは、内部メモリ、外部メモリ（メディア1、メディア2）のいずれかに格納されたデータファイルの読み出しに共通な処理フローである。図25において、左側がデバイスの制御部、右側がデバイスのメモリインタフェースの処理である。

【0152】

まず、制御部は、ファイル割り当てテーブル（図17参照）から読み出し対象データのセクタアドレス（S（1）～S（k））を取得（S501）し、メモリインタフェースに取得したセクタS（i）読み出しコマンドを順次送信（S502，S503）する。メモリインタフェースは、セクタS（i）読み出しコマンドを受信（S504）すると、ビジーフラグを1（ビジー）に設定（S505）し、受信セクタS（i）が内部メモリか、外部メモリであるかを判定（S506）し、外部メモリである場合は、メディア1かメディア2のセットフラグが1（メディアが有効にセットされていることを示す）であるかを判定（S507）し、セットフラグが1である場合には、さらにブロックパーミッション・テーブル（BPT）を参照して、BPTが読み出し対象であるセクタS（i）を読み出し許可対象ブロックとして設定しているかを判定（S508）する。BPTに読み出し許可ブロックの設定がある場合には、外部メモリから該当セクタのデータを読み出す（S509）。

【0153】

なお、読み出し対象データがBPTによる管理のなされていない内部メモリ内のデータである場合は、ステップS507、S508はスキップする。ステップS507、S508の判定がNoである場合、すなわちセクタS(i)を格納したメディアのセットフラグが1でない場合、または、BPTにセクタS(i)の読み出し許可が設定されていない場合には、ステップS513に進み、読み出しエラーとして読み出し成功フラグが0にセットされる。

【0154】

ステップS506～S508の判定ブロックにおいて、対象セクタS(i)の読み出しが実行可と判定されると、メモリから該当セクタが読み出され、セクタに対応して設定されている冗長部の誤り訂正符号に基づく誤り訂正処理が実行(S510)され、誤り訂正が成功した(S511)ことを確認し、読み出し成功フラグを1(成功)にセットし、読み出し結果をバッファに格納(S512)し、ビジーフラグを0(待機)に設定(S513)する。誤り訂正に失敗した場合は、読み出し成功フラグを0(失敗)に設定(S513)して処理を終了する。

【0155】

また、制御部は、ステップS515～S520において、メモリインタフェースのステータスを読み出して、ビジーフラグが0の状態において、読み出し成功フラグが1であることを条件として読み出しデータをバッファから取り出して保存し、アドレスを順次インクリメントして、データを順次バッファから取り出して保存する処理を繰り返し実行し、すべての読み出し対象セクタを保存した後、全読み出しセクタデータからファイルを構成して処理を終了する。

【0156】

(ファイル書き込み処理)

次に、データファイルの書き込み処理について図26のフローを用いて説明する。図26に示すフローは、内部メモリ、外部メモリ(メディア1、メディア2)のいずれかにファイルを書き込む際の共通処理フローである。図26において、左側がデバイスの制御部、右側がデバイスのメモリインタフェースの処理である。

【0157】

まず、制御部は、書き込み対象ファイルをセクタに分割する。分割されたデータをD(1)～D(k)とする。制御部は、次に各データD(i)の書き込みセクタS(i)を設定して、メモリインタフェースにセクタS(i)書き込みコマンドと、データD(i)を順次送信(S602～S604)する。メモリインタフェースは、セクタS(i)書き込みコマンドを受信(S605)すると、ビジーフラグを1(ビジー)に設定(S606)し、受信セクタS(i)が内部メモリか、外部メモリであるかを判定(S607)し、外部メモリである場合は、メディア1かメディア2のセットフラグが1(メディアが有効にセットされていることを示す)であるかを判定(S608)し、セットフラグが1である場合には、さらにブロックパーミッション・テーブル(BPT)を参照して、BPTが書き込み対象であるセクタS(i)を書き込み許可対象ブロックとして設定しているかを判定(S609)する。BPTに書き込み許可ブロックの設定がある場合には、セクタに対応して設定する誤り訂正符号を生成(S610)し、セクタS(i)にデータD(i)と誤り訂正符号を持つ冗長部を書き込み、書き込み成功フラグを1(成功)にセットし、ビジーフラグを0(待機)に設定(S614)する。

【0158】

なお、書き込み対象データがBPTによる管理のなされていない内部メモリ内への書き込み処理である場合は、ステップS608、S609はスキップする。ステップS608、S609の判定がNoである場合、すなわちメディアのセットフラグが1でない場合、または、BPTにセクタS(i)の書き込み許可が設定されていない場合には、ステップS613に進み、書き込みエラーとして書き込み成功フラグを0にセットする。

【0159】

また、制御部は、ステップS616～S620において、メモリインタフェースのステータスを読み出して、ビジーフラグが0の状態において、書き込み成功フラグが1であることを条件としてアドレスを順次インクリメントして、書き込みデータを順次メモリインタフェースに送信する。すべての処理が終了すると、

ファイル割り当てテーブルの更新処理を実行（S 6 2 1）し、更新したファイル割り当てテーブルを更新コマンドとともにメモリインタフェースに送信（S 6 2 2）し、メモリインタフェースはコマンドに従ってファイル割り当てテーブルの書き込み処理を実行（S 6 2 3）する。

【0160】

[セクタ位置に応じた暗号化鍵を適用した暗号化処理]

次に、セクタ位置に応じた暗号化鍵を適用した暗号化処理について説明する。著作権などを保護するためにコンテンツ部に対する暗号化を行う場合があるが、コンテンツ部全体に対して一つの暗号化鍵を使って暗号化すると、同一の鍵の元での大量の暗号文が発生し、攻撃が容易となってしまう危険性がある。通常はコンテンツ部をできるだけ分割し、それぞれを異なる鍵で暗号化する方が望ましいと言える。本システムでのコンテンツ暗号化の最小単位として、セクタが挙げられるが、ヘッダ領域に鍵を保存するという目的の場合には、セクタの数だけ8バイト（DESの場合）または16バイト（トリプルDES（Triple-DESの場合））の鍵情報が必要となるためヘッダのサイズが膨大になってしまい限られたメモリ領域のデータ領域を減少させてしまうことになり、実用上好ましくない。また、各セクタのデータ部分にそのセクタを暗号化するための鍵を格納する方法をとればヘッダサイズに影響を及ぼすことはないが、鍵の領域にはデータを置けなくなるためデータサイズが目減りしてしまうことと、万一、制御部側でファイルシステムを持つようなシステムの場合にはファイルシステム自体に大幅な変更を必要とする。

【0161】

そこで、本発明のシステムでは、先に説明した各コンテンツの属性情報であるセキュリティヘッダ（図7参照）の中に例えば、メディアの1ブロックあたりのセクタ数Mに対応するM個の鍵情報を格納し、これらを各セクタに対する暗号化鍵として適用する（図8参照）。図7に示したセキュリティヘッダ中のKc__Encrypted0～Kc__Encrypted31が32個の暗号化鍵Kcを示す。なお、[Encrypted]は、それぞれの鍵Kcが暗号化されて格納されていることを示す。これらの複数の鍵の中からセクタのブロック内位置によって鍵を選択してセクタ対応の

暗号化鍵として用いる構成とした。

【0162】

図27に、コンテンツのヘッダ情報としてコンテンツに対応して生成されるセキュリティヘッダにおける鍵格納構成と、各格納鍵と、各鍵の適用対象となるメモリ内の各セクタとの対応を説明する図を示す。図27(a)が先に図7を用いて説明したセキュリティヘッダ内の鍵格納構成を簡略化して示した図である。図27(a)のセキュリティヘッダには、 $K_c(0) \sim K_c(M-1)$ までのM個の鍵（コンテンツキー）が格納されている。ヘッダには鍵以外にもバージョン、コンテンツタイプ等の各種情報が格納され、さらにヘッダ情報の改竄チェック用のICVが格納されている。

【0163】

このM個のコンテンツキーは、例えば図27(b)に示すように各々が各セクタに対応付けられて各セクタに格納するデータの暗号化に使用される。先に図3を用いて説明したように、ブロック単位での消去を行なうフラッシュメモリは、図27(b)に示すようにデータ格納領域がブロック単位に分割され、各ブロックはさらに複数セクタに分割されている。例えば鍵 $K_c(0)$ を、メモリの各ブロックのセクタ0に格納するデータの暗号化鍵として適用し、鍵 $K_c(s)$ を、メモリの各ブロックのセクタsに格納するデータの暗号化鍵とする。さらに、鍵 $K_c(M-1)$ を、メモリの各ブロックのセクタM-1に格納するデータの暗号化鍵として適用する。

【0164】

このように、セクタに対応して異なる暗号鍵を適用してデータを格納することにより格納データ（ex. コンテンツ）のセキュリティが高められる。すなわち、コンテンツ全体を1つの鍵で暗号化した場合は、鍵漏洩によるコンテンツ全体の復号が可能となるのに対し、本構成によれば、1つの鍵の漏洩によってデータ全体を復号することは不可能であるからである。

【0165】

暗号化アルゴリズムは、例えば1つの暗号鍵によるDES暗号化処理を実行するシングルDESが適用される。また、シングルDESではなく、暗号化に2つ

以上の鍵を使用するトリプルDES (Triple DES) を適用した暗号化構成としてもよい。

【0166】

トリプルDES (Triple DES) の詳細構成例を図28に示す。図28 (a)、(b)に示すようにトリプルDES (Triple DES) としての構成には、代表的には以下のような2つの異なる態様がある。図28 (a)は、2つの暗号鍵を用いた例を示すものであり、鍵1による暗号化処理、鍵2による復号化処理、さらに鍵1による暗号化処理の順に処理を行う。鍵は、K1、K2、K1の順に2種類用いる。図28 (b)は3つの暗号鍵を用いた例を示すものであり、鍵1による暗号化処理、鍵2による暗号化処理、さらに鍵3による暗号化処理の順に処理を行い3回とも暗号化処理を行う。鍵は、K1、K2、K3の順に3種類の鍵を用いる。このように複数の処理を連続させる構成とすることで、シングルDESに比較してセキュリティ強度を向上させることが可能である。

【0167】

図29に、メモリに格納するデータの各セクタ毎に異なる2つの暗号鍵のペアを適用してトリプルDESによる暗号化処理を行なった構成例を示す。図29に示すように、各ブロックのセクタ0は、鍵Kc(0)とKc(1)の2つの鍵を用いてトリプルDES暗号化を行ない、セクタsは、鍵Kc(s)とKc(s+1)の2つの鍵を用いてトリプルDES暗号化を行ない、セクタM-1は、鍵Kc(M-1)とKc(0)の2つの鍵を用いてトリプルDES暗号化を行なう。この場合でも、ヘッダに格納する鍵数は、M個であり、図27(a)で示した鍵格納数を増加させる必要はなく、セキュリティを高めることが可能となる。

【0168】

さらに、図30に異なる態様でのデータ暗号化構成例を示す。図30は、メモリの各ブロックの2つの連続するセクタ領域を1つの暗号化ブロックとして、2つの鍵を用いてトリプルDES暗号化を行なった態様である。図30に示すように、各ブロックのセクタ0とセクタ1は、鍵Kc(0)とKc(1)の2つの鍵を用いてトリプルDES暗号化を行ない、セクタ2sとセクタ2s+1は、鍵Kc(2s)とKc(2s+1)の2つの鍵を用いてトリプルDES暗号化を行な

い、セクタ $M-2$ とセクタ $M-1$ は、鍵 $K_c(M-2)$ と $K_c(M-1)$ の2つの鍵を用いてトリプルDES暗号化を行なう。このように複数のセクタに同一の暗号化処理を適用することで暗号化プロセスまたは復号プロセスの処理軽減を可能とすることができる。

【0169】

図27、図29、図30に示す例の他にも、ヘッダに複数鍵を格納し、その複数鍵から選択した鍵を用いてセクタ毎の暗号化を実行する構成としては様々な構成が可能である。例えば、図27、29、30では、セクタ数と同数の鍵をヘッダに格納する構成としているが、例えばセクタ数が M のとき、格納鍵数を N ($N < M$)として、セクタ0とセクタ s は同じ鍵で暗号化する等の構成としてもよい。また格納鍵数を L ($L > M$)として、各セクタごとに全く異なる複数の鍵セットによるトリプルDESを適用する構成としてもよい。

【0170】

〔セクタ単位の改竄チェック値 (ICV) の付加構成〕

次に、セクタ単位の改竄チェック値 (ICV) の付加構成について説明する。複数セクタにまたがって構成されるデータについて、その正当性を確認する場合、一般には、コンテンツデータ全体の最後などに前述した改竄チェック値 (ICV) を付加させる構成とするのが一般的であった。このようなデータ全体のICVの付加構成においては、データを構成している各セクタ単位で、正当性を確認することができない。

【0171】

またICVを格納する場合、実データであるコンテンツの格納領域と同領域にICVを入れ込むと、その分データ部として使用できる領域が減ってしまう。もし、各セクタにセクタ内のデータに対してセクタ毎のICVを入れ込むと、デバイスのファイルシステムはデータ部単位でデータを読み出す処理を実行するために、実際に使用されるデータをICVから切り離して取り出すための処理、すなわち一度、読み出したデータ部内のセクタ内のICVを取り除く処理と、取り出したセクタ内のデータを複数セクタで連結する処理を実行することが必要となり、その処理を実行するためのファイルシステムを新たに構築することが必要とな

る。さらに、これらの I C V チェックを制御部で行うとなると、制御部にその処理の分の負荷がかかってしまう。

【 0 1 7 2 】

本発明のデータ処理装置においては、セクタ毎にデータ改竄チェックを可能とするため、セクタ毎に I C V を設定し、その I C V 設定位置を実データ領域ではなく、デバイスのファイルシステムによって読み取られない領域として予め設定されている冗長部領域とした。冗長部に I C V を置く構成とすることで、データ内に I C V を置く必要がなくなり、データ部の領域が多く利用できる。また、冗長部に I C V を置くことで、データ部と I C V の切り分け・データ連結処理が不要となるために、データ読み出しの連続性が保たれる。

【 0 1 7 3 】

データを読み出す時には、メモリアインタフェース部 3 0 0 (図 2 参照) でセクタ毎の I C V チェック処理を実行し、改竄ありと判定され無効なデータである場合は制御部 2 0 5 (図 2 参照) への転送を実行しない。また、データ書き込み時には、メモリアインタフェース部 3 0 0 において各セクタの I C V を計算して、冗長部に書きこむ処理を実行する。

【 0 1 7 4 】

なお、各セクタで I C V を付加するかしないかを、セキュリティヘッダ (Security Header) に記述して指定する。この構成については、図 7 のセキュリティヘッダ構成の説明中に示したように、セキュリティヘッダ中の I C V フラグ (I C V Flag) が、ブロック内のセクタ数 (32 セクタ) 分のフラグを持ち、ブロック内の各セクタの I C V 付加・非付加を示す。例えば 0 : I C V なし、1 : I C V あり、として設定される。

【 0 1 7 5 】

各セクタのデータ利用部と冗長部構成を図 3 1 に示す。図 3 1 (a) のように、メモリ (フラッシュメモリ) に格納されるデータは複数のセクタ領域を持つブロック単位領域に分割して格納される。(b) に示すように、各セクタはデバイスのファイルシステムによって実データ (e x. コンテンツ) として読み取られる例えば 5 1 2 あるいは 1 0 2 4 バイトのデータ利用部と、ファイルシステムに

よっては読み取られない E C C (Error Correction Code) 等の情報を格納した冗長部とによって構成される。

【0 1 7 6】

この冗長部の容量は例えば 1 6 バイト、あるいは 2 0 バイトの予め決められた領域であり、デバイスのファイルシステムは、この冗長部を非データ領域として認識し、データ（コンテンツ）読み取り処理においては読み取らない。一般に、冗長部に格納される E C C は、冗長部全体を使用せず、冗長部には非使用領域（リザーブ領域）が存在する。このリザーブ領域に各セクタの改竄チェック値（I C V）を格納する。

【0 1 7 7】

冗長部に I C V を格納した場合のデバイスのファイルシステムによるデータ部の連結処理は、図 3 1（c）に示すように、純粹にデータとして使用するものだけが格納されたデータ部の連結を行なうのみの従来のデータ連結処理と同様の処理が可能となる。従って、デバイスのファイルシステムは、冗長部を除くデータ部領域を単に連結すればよく、新たな処理は何ら必要としない。

【0 1 7 8】

本構成により、複数のセクタで構成されるデータのセクタ単位でデータの正当性の検証することが出来る。また、改竄チェック用の I C V を冗長部に入れることで、データ用に使えるデータ領域をそのまま活用することが出来る。また、制御部には、I C V チェックの結果、正しい（改竄なし）と判定された正しいセクタのみが送信される。また、I C V チェックがメモリインタフェース部にて行われるので、制御部の負担がかからない等の効果がある。

【0 1 7 9】

〔メディア内の個別鍵によるコンテンツ鍵の保存処理〕

次に、メディア内の個別鍵によるコンテンツ鍵の保存処理構成について説明する。先に、図 7 を用いて説明したように、コンテンツに対応して構成されるセキュリティヘッダには、セクタ対応の暗号鍵としての複数のコンテンツキー（K c __Encryptedxx）、およびコンテンツチェック値生成鍵（K i c v __Encrypted）が暗号化されて格納されている。

【0180】

これらの鍵の暗号化の1つの態様は、予めデバイスのメモリインタフェースのメモリ部321（図4参照）に格納されている配送鍵 K_{dist} によって暗号化して格納する構成がある。例えば、 $K_{c_Encrypted0} = Enc(K_{dist}, K_c(0))$ である。ここで、 $Enc(a, b)$ は、 b を a で暗号化したデータであることを示す。このように、それぞれの鍵をデバイスの配送鍵 K_{dist} を用いて暗号化してセキュリティヘッダに格納する構成が1つの構成である。

【0181】

さらに、メディア2、すなわち暗号処理部を持ち、デバイスとの相互認証を実行してコンテンツ処理を実行するメディアにおいて、メディア2の固有鍵を用いてメディア2に格納するコンテンツに関するコンテンツキー、ICV生成鍵を暗号化する態様がある。以下、メディア2の固有鍵、ここではメディア2保存鍵 K_{sto} を用いて暗号化したコンテンツキー、コンテンツICV生成鍵をセキュリティヘッダに格納する処理について説明する。

【0182】

メディア2保存鍵 K_{sto} は、図2に示したようにメディア2、230のメディア2コントローラ231の内部メモリ235に格納されている。従って、メディア2保存鍵 K_{sto} を使用したコンテンツキー、ICV生成鍵の暗号化処理、復号処理はメディア2側で実行される。メディア2を装着したデバイスが、メディア2のコンテンツ利用に際し、コンテンツキー、ICV生成鍵を取得、あるいはセキュリティヘッダへの格納処理を実行する場合は、メディア2側で鍵の暗号化、復号処理を実行することが必要となる。本発明のデータ処理装置においては、これらをCBC（Cipher Block Chaining）モードで処理することを可能とした。

【0183】

図32にCBCモードにおける鍵の暗号化処理構成を示す。この暗号化処理は、メディア2の暗号処理部236（図2参照）において実行される。内部メモリ235に格納された初期値 IV_keys と、コンテンツチェック値生成鍵 K_{icv_cont} との排他論理和を実行し、その結果をメディア2の内部メモリ235に格

納された保存鍵K s t oを適用したD E S暗号化を行ない、その結果をK i c v _cont Encryptedとしてヘッダに格納する。さらに、K i c v _cont Encryptedと、セクタ(0)に対応するセクタ対応コンテンツキーK c (0)との排他論理和を実行し、その結果をメディア2の内部メモリ235に格納された保存鍵K s t oを適用したD E S暗号化を行ない、その結果をK c (0) Encryptedとしてヘッダに格納する1つの暗号化コンテンツキーとする。さらに、K c (0) Encryptedと、セクタ(1)に対応するセクタ対応コンテンツキーK c (1)との排他論理和を実行し、その結果に対して保存鍵K s t oを適用したD E S暗号化を行ない、その結果をK c (1) Encryptedとする。以下、これらの処理を繰り返し実行して、ヘッダ格納用の鍵データとする。

【0184】

次に、図33にC B Cモードにおける鍵の復号処理構成を示す。この復号処理は、メディア2の暗号処理部236(図2参照)において実行される。まず、K c (0) Encryptedに対して、メディア2の内部メモリ235に格納された保存鍵K s t oを適用したD E S復号処理を行ない、その結果を内部メモリ235に格納された初期値I V _keysと排他論理和することにより、セクタ(0)に対応するセクタ対応コンテンツキーK c (0)が出力される。さらに、K c (1) Encryptedに対して、保存鍵K s t oを適用したD E S復号処理を行ない、その結果をコンテンツキーK c (0) Encryptedと排他論理和することにより、セクタ(1)に対応するセクタ対応コンテンツキーK c (1)が出力される。以下、これらの処理を繰り返し実行して、コンテンツキーを取得する。なお、図には、コンテンツキーのみを出力データとした例を示しているが、コンテンツ改竄チェック値生成鍵(K i c v _Encrypted)についても同様の処理が適用可能であり、暗号化されたコンテンツ改竄チェック値生成鍵(K i c v _Encrypted)からコンテンツ改竄チェック値生成鍵(K i c v)の生成が可能である。

【0185】

上述のセクタ対応コンテンツキーK c (x x)またはコンテンツ改竄チェック値生成鍵(K i c v)の暗号化、復号処理は、多くの場合、メディア2を装着したデバイスからのコマンドに基づいて実行される。この場合、デバイスとメディ

ア2間では前述した相互認証が実行され、相互認証処理が成立したことを条件としてコンテンツ再生、格納等の様々な処理が実行され、その一連のコンテンツ処理の1つとして上述のコンテンツキーの復号、暗号化処理が実行されることになる。復号された鍵（ex. コンテンツキー $K_c(x)$ ）をデバイスとメディア2間において転送する場合は、相互認証時に生成したセッションキー K_{ses} で暗号化される。このセッションキー K_{ses} による暗号化、復号処理もCBCモードを適用することで、よりセキュリティを高めることが可能となる。

【0186】

図34にメディア2において、セキュリティヘッダに格納された鍵をDES-CBCモードで復号し、復号した鍵データをさらにセッションキー K_{ses} を適用してDES-CBCモードで暗号化する処理構成を示す。図34の上段は、図33と同様の構成であり、セキュリティヘッダから取り出した暗号化されたコンテンツキーを順次DES復号部に入力してメディア2の保存鍵 K_{sto} を適用して復号処理を実行し、出力結果を初期値、または入力データ列の前データと排他論理和して、出力結果としてのコンテンツキーを取得する。

【0187】

これらの出力された結果をさらに、デバイスとの相互認証時に生成したセッションキー K_{ses} を適用したDES-CBCモードでの暗号化処理を実行する。その結果得られた $SE0 \sim SEM-1 : K_c(0) \text{ Encrypted} \sim K_c(M-1) \text{ Encrypted}$ をデバイスに送信する。デバイス側では、受信したデータ列 $K_c(0) \text{ Encrypted} \sim K_c(M-1) \text{ Encrypted}$ について、メディア2との相互認証時に生成したセッションキー K_{ses} を適用して、図33と同様のDES-CBCモードでの復号処理を実行することによりコンテンツキー $K(c)$ を取得することができる。なお、図には、コンテンツキーのみを処理データとした例を示しているが、コンテンツ改竄チェック値生成鍵($K_{icv_Encrypted}$)についても同様に処理データとして構成することが可能である。

【0188】

[暗号化データの読み出し処理]

図35以下のフローを用いて、暗号化されたデータのメディアからの読み出し

処理の詳細を説明する。なお、データの暗号化態様は、上述したようにセクタ毎に異なる鍵で暗号化した態様と、コンテンツ全体を1つの暗号化鍵で暗号化した態様とがあり、これらは、ヘッダの情報に基づいて判定される。図35のフローにおいて左側はデバイスの制御部、右側はデバイスのメモリインタフェースの処理である。

【0189】

まず制御部は、読み出し対象となるコンテンツのヘッダファイルを読み出す（S701）。この処理は、前述の図25のファイル読み出し処理フローに従った処理として実行される。次にヘッダセットコマンドと、読み出したヘッダファイルをメモリインタフェースに送信（S702）する。

【0190】

メモリインタフェースはヘッダセットコマンドを受信（S703）すると、ビジーフラグを1（ビジー）にセット（S704）し、ヘッダの改竄チェック値（ICV）を検証（S705）する。ヘッダのICVチェックは、先に図14を用いて説明したICV生成処理において、セキュリティヘッダ検証値生成鍵Kicv__shと、初期値IVshを適用してヘッダの構成データを入力してICV'を生成し、生成したICV'と予めヘッダに格納されたICVとを照合する処理によって実行する。

【0191】

検証によりヘッダ改竄なしと判定（S706）されると、ヘッダ内の有効リボケーションリスト・バージョンが0でないかがチェック（S707）される。例えば、自デバイスで生成し格納したコンテンツをメモリに格納するとき等は、リボケーションリスト・バージョンを0として、再生処理等の際にリボケーションリストを非参照とした処理を実行可能とする。

【0192】

リボケーションリスト・バージョンが0の場合は、リボケーションリストを参照する必要がないのでステップS710に進む。バージョンが非0であるときは、現在セットされているリボケーションリストが、ヘッダのバージョンより古くないかをチェック（S708）し、古い場合は、S713に進み、ヘッダセット

成功フラグを 0 (NG) に設定して処理を終了する。セットされているリボケーションリストがヘッダのバージョンより古くなければ、ステップ S 7 0 9 に進み、リボケーションリストを参照して、読み出し対象のコンテンツ ID がないかを判定する。あった場合は読み出しを禁止する処理として、ステップ S 7 1 3 でヘッダセット成功フラグを 0 (NG) として処理を終了する。

【 0 1 9 3 】

リボケーションリストに読み出し対象コンテンツ ID が記録されていないならば、ステップ S 7 1 0 に進み、ヘッダ情報に基づいて暗号化されたコンテンツキー K_c と、コンテンツチェック値生成鍵 K_{icv}__cont を復号する。なお、リボケーションリストは、先の図 1 6 の起動時フローにおいて説明したように、起動時にメモリインタフェースにセットアップされ、セットアップ後は、メディアの装着時、コンテンツの再生時においてメモリインタフェースにおいて継続的に利用可能としたリボケーションリストである。

【 0 1 9 4 】

先に、図 7 他を用いて説明したようにセキュリティヘッダの中には、前述のセクタ毎に適用する暗号鍵としての複数のコンテンツキー K_c (0) ~ K_c (M-1) が暗号化されて格納されている。また、コンテンツの改竄チェック値 (ICV) を生成するためのコンテンツチェック値生成鍵 K_{icv}__cont も暗号化されて格納されている。

【 0 1 9 5 】

コンテンツの復号に先立ち、これらのコンテンツチェック値生成鍵 K_{icv}__cont を復号してコンテンツの改竄チェックを実行する処理が必要であり、また、コンテンツキー K_c (0) ~ K_c (M-1) を復号する処理が必要となる。

【 0 1 9 6 】

図 3 7 に暗号化されたコンテンツキー K_c、コンテンツチェック値生成鍵 K_{icv}__cont の復号処理フローを示す。図 3 7 の各ステップについて説明する。図 3 7 の処理は、デバイスのメモリインタフェースにおける処理である。図 4 の暗号処理部 3 2 0 において実行される。

【 0 1 9 7 】

まず、暗号化コンテンツチェック値生成鍵 K_{icv_cont} を復号対象として選定 (S 8 0 1) し、次に、ヘッダの暗号化フォーマットタイプ・フィールドの設定が 0 か否かを判定 (S 8 0 2) する。暗号化フォーマットが 0 である場合は、コンテンツ全体をセクタに係わらず 1 つの暗号化態様としたデータ構成であり、暗号化フォーマットタイプ・フィールドの設定が 1 である場合は、前述の図 2 7 他で説明したセクタ単位の暗号化鍵を用いた方法である。セクタ単位の暗号化鍵を用いた方法である場合は、ステップ S 8 0 3 に進み、セクタ毎に設定された暗号化コンテンツキー ($K_{c_Encrypted0 \sim 31}$) を復号対象にする。

【 0 1 9 8 】

ステップ S 8 0 2 で暗号化フォーマットが 0 であると判定された場合は、ステップ S 8 0 4 でさらに、ヘッダの暗号化アルゴリズムフィールドをチェックして 1 (トリプル DES) が 0 (シングル DES) であるかを判定する。シングル DES である場合は、ステップ S 8 0 5 で 1 つの暗号化コンテンツキー ($K_{c_Encrypted0}$) のみを復号対象として加え、トリプル DES である場合は、ステップ S 8 0 6 で複数の暗号化コンテンツキー ($K_{c_Encrypted0, 1}$) を復号対象として加える。

【 0 1 9 9 】

次に、ステップ S 8 0 7 において、ヘッダのコンテンツタイプフィールドの設定をチェックし、設定が 2 または 3 (メディア 2 の格納コンテンツ) でない場合は、ステップ S 8 0 8 で、メモリ部 3 2 1 (図 4 参照) に格納された配送鍵 K_{dist} で復号対象データ、すなわち、暗号化コンテンツチェック値生成鍵 K_{icv_cont} と、1 以上のコンテンツキーを復号する。

【 0 2 0 0 】

設定が 2 または 3 (メディア 2 の格納コンテンツ) である場合は、ステップ S 8 0 9 で復号対象データ、すなわち、暗号化コンテンツチェック値生成鍵 K_{icv_cont} と、1 以上のコンテンツキーをメディア 2 の保存鍵 K_{sto} (CBC モード) で復号する。この復号処理の詳細は、図 3 2、図 3 3、図 3 4 を用いて説明した通りである。

【 0 2 0 1 】

ステップS809におけるメディア2の保存鍵による暗号化コンテンツチェック値生成鍵 K_{icv_cont} と、1以上のコンテンツキー K_c の復号処理について図38のフローを用いて説明する。図38のフローは、左側にデバイスのメモリインタフェース、右側にメディア2のコントローラ（図2参照）の処理を示している。

【0202】

まず、メモリインタフェースは、復号対象データ $K(0) \sim K(n-1)$ （暗号化コンテンツチェック値生成鍵 K_{icv_cont} と、1以上のコンテンツキー）を設定（S1001）し、CBC復号初期化コマンドをメディア2コントローラに送信（S1003）し、メディア2コントローラはIVKeysをレジスタにセット（S1005）する。その後、メモリインタフェースは、各鍵を順次送信（S1004）し、メディア2コントローラが復号対象データ $K(i)$ を受信（S1005）する。

【0203】

次にメディア2コントローラは、受信した復号対象データ $K(i)$ に対して、メディア2の保存鍵 K_{sto} を用いたCBCモードによる復号処理を実行（S1007）し、復号された鍵データ（ex. 複数のセクタ対応コンテンツキー）を取得（S1008）する。次に、メディア2コントローラは、復号鍵データ列を、デバイスとの相互認証時に生成したセッションキーによってCBCモードでの暗号化処理を実行し、データ列 $K'(i)$ を生成して、結果をデバイスに送信（S1009）する。ステップS1007～S1009の処理は、先に説明した図34のDES-CBCモードによる処理に基づいて実行される。

【0204】

デバイスのメモリインタフェースは、順次 $K'(i)$ を受信し、すべてのデータを受信したことを確認の後、CBC終了コマンドをメディア2コントローラに送信する。メディア2コントローラはCBC終了コマンドの受信によりレジスタをクリア（S1014）する。

【0205】

デバイスのメモリインタフェースは、メモリ部321（図4参照）に格納した

初期値 I V_keys を用い、メディア 2 との相互認証時に生成したセッションキー Kses を適用して CBC モードでメディア 2 から受信した K' (i) を復号 (S1010 ~ S1013, S1015) する。この復号処理は、先に説明した図 33 の構成と同様の処理である。

【0206】

上記処理により、デバイスは、ヘッダに格納された暗号化されたコンテンツキー Kc、コンテンツチェック値生成鍵 Kicv_cont を復号し、それぞれの鍵を取得することができる。

【0207】

次に図 35 に戻り、暗号化ファイルの読み出し処理の続きを説明する。上記の鍵復号処理ステップであるステップ S710 を終了すると、ステップ S711 に進む。ステップ S711 では、デバイスのメモリインタフェースはヘッダを「読み出しヘッダ」として内部に設定し、ヘッダセット成功フラグを 1 (成功) にセットし、ビジーフラグを 0 (待機) (S714) 設定する。コンテンツ読み出しに際しては、設定されたヘッダの情報に基づく処理が実行される。

【0208】

一方、制御部側は、ステップ S715 でステータス読み出しコマンドをメモリインタフェースに送信し、ビジーフラグが 0 (待機) (S716) であり、ヘッダセット成功フラグが 1 (成功) (S717) となったことを条件として次の処理 (図 36) に進む。

【0209】

図 36 のステップ S721 において、制御部は、ファイル割り当てテーブルから読み出し対象のコンテンツファイルのセクタアドレス (S(1) ~ S(k)) を取得し、メモリインタフェースに対して順次、セクタ S(i) 読み出しコマンドを送信する。

【0210】

メモリインタフェースは、セクタ S(i) 読み出しコマンドを受信 (S724) すると、ビジーフラグを 1 (ビジー) に設定 (S725) し、ヘッダ成功フラグが 1 (成功) であることを条件 (S726) として次ステップに移行する。ヘ

ッダ成功フラグが1（成功）でない場合は、ステップS 7 3 8に進み、読み出し成功フラグを0（NG）として処理を終了する。

【0 2 1 1】

ヘッダ成功フラグが1（成功）である場合は、受信セクタS（i）が内部メモリか、外部メモリであるかを判定（S 7 2 7）し、外部メモリである場合は、メディア1かメディア2のセットフラグが1（メディアが有効にセットされていることを示す）であるかを判定（S 7 2 8）し、セットフラグが1である場合には、さらにブロックパーミッション・テーブル（BPT）を参照して、BPTが読み出し対象であるセクタS（i）を読み出し許可対象ブロックとして設定しているかを判定（S 7 2 9）する。BPTに読み出し許可ブロックの設定がある場合には、外部メモリから該当セクタのデータを読み出す（S 7 3 0）。

【0 2 1 2】

なお、読み出し対象データがBPTによる管理のなされていない内部メモリ内のデータである場合は、ステップS 7 2 8、S 7 2 9はスキップする。ステップS 7 2 8、S 7 2 9の判定がNoである場合、すなわちセクタS（i）を格納したメディアのセットフラグが1でない場合、または、BPTにセクタS（i）の読み出し許可が設定されていない場合には、ステップS 7 3 8に進み、読み出しエラーとして読み出し成功フラグが0にセットされる。

【0 2 1 3】

ステップS 7 2 6～S 7 2 9の判定ブロックにおいて、対象セクタS（i）の読み出しが実行可と判定されると、メモリから該当セクタが読み出され、セクタに対応して設定されている冗長部の誤り訂正符号に基づく誤り訂正処理が実行（S 7 3 1）され、誤り訂正が成功した（S 7 3 2）ことを確認する。次に、ヘッダのICVフラグ（図7参照）を参照し、読み出し対象セクタが改竄チェック値（ICV）による処理対象であるかを判定する。先に図3 1を用いて説明したように各セクタは、その冗長部に改竄チェック用のICVを格納しており、セクタ単位での改竄チェックが可能である。

【0 2 1 4】

ICVによる改竄チェックの対象である場合は、ステップS 7 3 4において、

ステップ S 7 1 0 の復号処理によって得たコンテンツチェック値生成鍵 K_{icv_cont} と、初期値 IV_{cont} を適用し改竄チェック対象データ（セクタデータ）を入力して図 1 4 を用いて説明した I C V 生成処理を実行し、 ICV' を求め、セクタの冗長部に格納されている I C V との照合を行ない一致していれば改竄なしと判定する。

【 0 2 1 5 】

I C V チェックにより改竄なしと判定されると、ステップ S 7 3 7 に進み、ヘッダ情報に基づいてデータの復号処理を実行して読み出し成功フラグを 1（成功）に設定し、復号データをバッファに格納する。

【 0 2 1 6 】

また、制御部は、ステップ S 7 4 0 ～ S 7 4 6 において、メモリインタフェースのステータスを読み出して、ビジーフラグが 0 の状態において、読み出し成功フラグが 1 であることを条件として読み出しデータをバッファから取り出して保存し、アドレスを順次インクリメントして、データを順次バッファから取り出して保存する処理を繰り返し実行し、すべての読み出し対象セクタを保存した後、全読み出しセクタデータからファイルを構成して処理を終了する。

【 0 2 1 7 】

図 3 6 のステップ S 7 3 6 のデータ部復号処理の詳細を図 3 9 を用いて説明する。この復号処理はデバイスのメモリインタフェースの暗号処理部 3 2 0（図 4 参照）において実行される。

【 0 2 1 8 】

まず、復号対象のデータ格納セクタ位置を s ($0 \leq s \leq 31$ （セクタ数 32 の場合）) とする (S 1 1 0 1)。次にそのセクタが暗号化対象であるかをチェック (S 1 1 0 2) する。このチェックは、セキュリティヘッダ（図 7 参照）の暗号化フラグ (Encryption Flag) に基づいて判定される。暗号化対象でない場合は、復号処理は実行されず、処理は終了する。暗号化対象である場合は、暗号化フォーマットタイプをチェック (S 1 1 0 3) する。これはセキュリティヘッダ内の暗号化フォーマットタイプ (Encryption Format Type) の設定をチェックするものであり、図 8 で説明したコンテンツ全体を 1 つの暗号化態様としているか

、各セクタに異なる鍵を用いた暗号化処理を行なっているかを判定する。

【0219】

暗号化フォーマットタイプ (Encryption Format Type) の設定値が0の場合は、コンテンツ全体を1つの暗号化態様としている場合である。この場合は、ステップS1104において、暗号化アルゴリズム (Encryption Algorithm) の判定を行なう。暗号化アルゴリズムは、シングルDESかトリプルDES (図28参照) かを設定しているものであり、シングルDESであると判定された場合は、1つのコンテンツキー $K_c(0)$ を適用して暗号化コンテンツの復号処理を実行 (S1106) する。トリプルDESであると判定された場合は、2つのコンテンツキー $K_c(0)$ 、 $K_c(1)$ を適用して暗号化コンテンツの復号処理を実行 (S1107) する。

【0220】

一方、ステップS1103で、暗号フォーマットタイプ (Encryption Format Type) の設定値が1の場合は、各セクタに異なる鍵を用いた暗号化処理を行なっている場合である。この場合は、ステップS1105において、暗号化アルゴリズム (Encryption Algorithm) の判定を行なう。暗号化アルゴリズムは、シングルDESかトリプルDES (図28参照) かを設定しているものであり、シングルDESであると判定された場合は、各セクタ (s) に対応して設定されたコンテンツキー $K_c(s)$ を各セクタに適用して暗号化コンテンツの復号処理を実行 (S1108) する。トリプルDESであると判定された場合は、2つのコンテンツキー $K_c(s)$ 、 $K_c(s+1 \bmod 32)$ を適用して各セクタ毎の暗号化コンテンツの復号処理を実行 (S1109) する。

【0221】

セクタデータの復号処理の異なる処理態様を図40に示す。図40において、ステップS1201～S1208は、図39の各ステップS1101～S1108と同様である。ステップS1209～S1211が図39とは異なる。

【0222】

ステップS1205において、暗号化アルゴリズムがトリプルDESであると判定された場合、ステップS1209においてセクタNo. (s) を判定し、s

が奇数である場合は、 $s = s - 1$ の更新を実行（S 1 2 1 0）し、各セクタに適用する鍵を $K_c(s)$ 、 $K_c(s+1)$ としてトリプルDESによる復号処理（S 1 2 1 1）を実行する。

【0223】

以上、暗号化されて格納されたデータの復号処理を伴う再生処理は、図35～図40を用いて説明したようなプロセスにより実行される。

【0224】

【データの暗号化書き込み処理】

次に、図41以下のフローを用いて、メディアに対するデータの暗号化書き込み処理プロセスの詳細を説明する。なお、データの暗号化態様は、上述したようにセクタ毎に異なる鍵で暗号化した態様と、コンテンツ全体を1つの暗号化鍵で暗号化した態様とがある。これらは、ヘッダ情報に設定される。図41のフローにおいて左側はデバイスの制御部、右側はデバイスのメモリアンタフェースの処理である。

【0225】

まず制御部は、読み出し対象となる格納コンテンツに対応するヘッダ生成コマンドとヘッダ情報としてのパラメータをメモリアンタフェースに送信する。（S 1 3 0 1）。

【0226】

メモリアンタフェースはヘッダ生成コマンドを受信（S 1 3 0 2）すると、ビジーフラグを1（ビジー）にセット（S 1 3 0 3）し、受信パラメータが許容値内であるかを判定（S 1 3 0 4）する。メモリアンタフェースは、予めヘッダに設定可能なパラメータ範囲を有しており、受信パラメータと比較し、受信パラメータが設定可能範囲を超えている場合は、ステップS 1 3 1 0においてヘッダ生成成功フラグを0（NG）に設定して処理を終了する。受信パラメータが許容値内である場合は、ヘッダの有効リボケーションリストバージョンを0に設定（S 1 3 0 5）し、リボケーションリストの非参照でのデータ処理を可能とする。有効リボケーションリストバージョンを0として設定するのは、自デバイスでの格納処理を行なったコンテンツについては正当なコンテンツであることが保証され

ているとの前提により、リボケーションリストの非参照でのデータ処理（再生）を可能とする設定を行なうものである。

【0227】

なお、書き込みコンテンツが例えば通信手段を介して外部から受信したコンテンツであり、受信コンテンツに識別子が付加され参照すべきリボケーションリストバージョンをヘッダに格納しておりデバイス内部のリボケーションリストとの照合が可能であれば、上記処理の代わりに、先に図35を用いて説明したファイル復号読み出し処理において実行されるステップS707～S709と同様のリボケーションリストを用いた識別子照合処理を行なってもよい。

【0228】

次に、ステップS1306において、ヘッダ情報に基づいてコンテンツキーK_c、コンテンツ改竄チェック値（ICV）生成鍵K_{icv_cont}を生成、暗号化する。ステップS1306のコンテンツキーK_c、コンテンツ改竄チェック値生成鍵K_{icv_cont}を生成、暗号化処理の詳細を図43に示す。図43の処理は、デバイスのメモリインタフェースの暗号処理部320（図4参照）において実行される。図43のフローについて説明する。

【0229】

まず、暗号化コンテンツチェック値生成鍵K_{icv_cont}を、例えば乱数に基づいて生成し、暗号化対象とし（S1401）、次に、ヘッダの暗号化フォーマットタイプ・フィールドの設定が0か否かを判定（S1402）する。暗号化フォーマットが0である場合は、コンテンツ全体をセクタに係わらず1つの暗号化態様とする構成であり、暗号化フォーマットタイプ・フィールドの設定が1である場合は、前述の図27他で説明したセクタ単位の暗号化鍵を用いる方法である。セクタ単位の暗号化鍵を用いる場合は、ステップS1403に進み、セクタ毎に設定されたコンテンツキー（K_c（0）～K_c（31）（セクタ数32の場合））を生成して暗号化対象とする。

【0230】

ステップS1404で暗号化フォーマットが0であると判定された場合は、ステップS1404でさらに、ヘッダの暗号化アルゴリズムフィールドをチェック

して1（トリプルDES）か0（シングルDES）であるかを判定する。シングルDESである場合は、ステップS1405で1つのコンテンツキー（ $K_c(0)$ ）を生成して暗号化対象として加え、トリプルDESである場合は、ステップS1406で複数のコンテンツキー（ $K_c(0)$ 、 $K_c(1)$ ）を生成して暗号化対象として加える。

【0231】

次に、ステップS1407において、ヘッダのコンテンツタイプフィールドの設定をチェックし、設定が2または3（メディア2の格納コンテンツ）でない場合は、ステップS1408で、メモリ部321（図4参照）に格納された配送鍵 K_{dist} でデータ、すなわち、コンテンツチェック値生成鍵 K_{icv_cont} と、1以上のコンテンツキーを暗号化する。

【0232】

設定が2または3（メディア2の格納コンテンツ）である場合は、ステップS1409でデータ、すなわち、コンテンツチェック値生成鍵 K_{icv_cont} と、1以上のコンテンツキーをメディア2の保存鍵 K_{sto} （CBCモード）で暗号化する。この暗号化処理の詳細は、図32、図33、図34を用いて説明した通りである。

【0233】

ステップS1409におけるメディア2の保存鍵によるコンテンツチェック値生成鍵 K_{icv_cont} と、1以上のコンテンツキー K_c の暗号化処理について図44のフローを用いて説明する。図44のフローは、左側にデバイスのメモリインタフェース、右側にメディア2のコントローラ（図2参照）の処理を示している。

【0234】

まず、デバイス側のメモリインタフェースは、暗号化対象データ $K(0) \sim K(n-1)$ （コンテンツチェック値生成鍵 K_{icv_cont} と、1以上のコンテンツキー）を設定（S1501）し、メディア2との相互認証時に生成したセッションキーを適用し、メモリ部321に格納した初期値 IV_keys を用いてDES-CBCモードによる暗号化対象データ $K(0) \sim K(n-1)$ の暗号化を実行

し、データ $K'(0) \sim K'(n-1)$ を生成(S1502)する。この暗号化処理は、先に説明した図32と同様の処理構成において実行される。次に、メモリインタフェースは、CBC暗号化初期化コマンドをメディア2コントローラに送信する。メディア2は、メディア2の内部に格納している初期値 IV_keys をレジスタにセット(S1506)する。その後、メモリインタフェースは、各鍵を順次送信(S1505)する。

【0235】

メディア2コントローラは、データ $K'(i)$ を受信(S1507)し、受信したデータ $K'(i)$ に対して、デバイスとの相互認証時に生成したセッションキーによってCBCモードでの復号処理を実行(S1508)し、復号された鍵データ(ex. 複数のセクタ対応コンテンツキー)を取得(S1509)する。次に、メディア2コントローラは、復号鍵データ列を、メディア2の保存鍵 K_{sto} を用いたCBCモードによる暗号化処理を実行し、データ列 $K''(i)$ を生成して、結果をデバイスに送信(S1510)する。ステップS1507～S1510の処理は、先に説明した図34のDES-CBCモードによる処理に基づいて実行される。

【0236】

デバイスのメモリインタフェースは、順次 $K''(i)$ を受信し、すべてのデータを受信したことを確認の後、CBC終了コマンドをメディア2コントローラに送信(S1511～S1514)する。メディア2コントローラはCBC終了コマンドの受信によりレジスタをクリア(S1515)する。

【0237】

デバイスのメモリインタフェースは、メディア2から受信した $K''(0) \sim K''(n-1)$ をヘッダ格納用の暗号化鍵データとする。上記処理により、デバイスは、ヘッダに格納する暗号化されたコンテンツキー K_c 、コンテンツチェック値生成鍵 K_{icv_cont} を取得することができる。

【0238】

図41に戻り、ファイルの暗号化書き込み処理の説明を続ける。ステップS1306において、上述のヘッダ格納鍵の生成、暗号化が終了すると、メモリイン

タフェースは生成したヘッダデータに基づく改竄チェック値 I C V を生成 (S 1 3 0 7) する。セキュリティヘッダのチェック値である I C V _ s h は、メモリ部 3 2 1 (図 4 参照) に格納された初期値 I V s h と、セキュリティヘッダ改竄チェック値生成鍵 K i c v _ s h を用いて、先に図 1 4 を用いて説明した I C V 生成構成に基づいて生成される。次に、ステップ S 1 3 0 8 で、生成されたヘッダを書き込みヘッダとして内部に保存し、ステップ S 1 3 0 9 でヘッダ生成成功フラグを 1 (成功) としてビジーフラグを 0 (待機) として処理を終了する。

【0239】

一方、制御部側は、ステップ S 1 3 1 2 でステータス読み出しコマンドをメモリインタフェースに送信し、ビジーフラグが 0 (待機) (S 1 3 1 3) であり、ヘッダ生成成功フラグが 1 (成功) (S 1 3 1 4) となったことを条件として、バッファからヘッダを読み出し、通常のファイルとしてメディアに保存 (S 1 3 1 5) 後、次の処理 (図 4 2) に進む。

【0240】

図 4 2 のステップ S 1 3 2 1 において、制御部は、書き込み対象のコンテンツファイルをセクタに分割する。分割されたデータを D (1) ~ D (k) とする。制御部は、次に各データ D (i) の書き込みセクタ S (i) を設定して、メモリインタフェースにセクタ S (i) の暗号化書き込みコマンドと、データ D (i) を順次送信 (S 1 3 2 1 ~ S 1 3 2 4) する。メモリインタフェースは、セクタ S (i) 暗号化書き込みコマンドを受信 (S 1 3 2 5) すると、ビジーフラグを 1 (ビジー) に設定 (S 1 3 2 6) し、ヘッダ生成成功フラグが 1 (成功) である (S 1 3 2 7) ことを条件として次ステップに進む。

【0241】

次に、メモリインタフェースは、受信セクタ S (i) が内部メモリか、外部メモリであるかを判定 (S 1 3 2 8) し、外部メモリである場合は、メディア 1 かメディア 2 のセットフラグが 1 (メディアが有効にセットされていることを示す) であるかを判定 (S 1 3 2 9) し、セットフラグが 1 である場合には、さらにブロックパーミッション・テーブル (B P T) を参照して、B P T が書き込み対象であるセクタ S (i) を書き込み許可対象ブロックとして設定しているかを判

定(S1330)する。BPTに書き込み許可ブロックの設定がある場合には、セクタに対応して設定する誤り訂正符号を生成(S1331)する。

【0242】

次に、その書き込みセクタがICV設定セクタであるか否かをヘッダ情報(ICVフラグ)に基づいて判定(S1332)し、ICV対象である場合は、コンテンツICV生成鍵 K_{icv_cont} に基づいてセクタデータに対するICVを生成(S1333)する。

【0243】

次に、メモリインタフェースは、ヘッダ情報に基づくデータの暗号化を実行(S1334)する。ステップS1334のデータ部暗号化処理の詳細を図45を用いて説明する。この暗号化処理はデバイスのメモリインタフェースの暗号処理部320(図4参照)において実行される。

【0244】

まず、暗号化対象のデータ格納セクタ位置を s ($0 \leq s \leq 31$ (セクタ数32の場合))とする(S1601)。次にそのセクタが暗号化対象であるかをチェック(S1602)する。このチェックは、セキュリティヘッダ(図7参照)の暗号化フラグ(Encryption Flag)に基づいて判定される。暗号化対象でない場合は、暗号化処理は実行されず、処理は終了する。暗号化対象である場合は、暗号化フォーマットタイプをチェック(S1603)する。これはセキュリティヘッダ内の暗号化フォーマットタイプ(Encryption Format Type)の設定をチェックするものであり、図8で説明したコンテンツ全体を1つの暗号化態様としているか、各セクタに異なる鍵を用いた暗号化処理を行なっているかを判定する。

【0245】

暗号化フォーマットタイプ(Encryption Format Type)の設定値が0の場合は、コンテンツ全体を1つの暗号化態様としている場合である。この場合は、ステップS1604において、暗号化アルゴリズム(Encryption Algorithm)の判定を行なう。暗号化アルゴリズムは、シングルDESかトリプルDES(図28参照)かを設定しているものであり、シングルDESであると判定された場合は、1つのコンテンツキー $K_c(0)$ を適用して暗号化コンテンツの暗号化処理を実

行(S1606)する。トリプルDESであると判定された場合は、2つのコンテンツキー $K_c(0)$ 、 $K_c(1)$ を適用して暗号化コンテンツの暗号化処理を実行(S1607)する。

【0246】

一方、ステップS1603で、暗号フォーマットタイプ(Encryption Format Type)の設定値が1の場合は、各セクタに異なる鍵を用いた暗号化処理を行なう場合である。この場合は、ステップS1605において、暗号化アルゴリズム(Encryption Algorithm)の判定を行なう。暗号化アルゴリズムは、シングルDESかトリプルDES(図28参照)かを設定しているものであり、シングルDESであると判定された場合は、各セクタ(s)に対応して設定されたコンテンツキー $K_c(s)$ を各セクタに適用して暗号化コンテンツの暗号化処理を実行(S1608)する。トリプルDESであると判定された場合は、2つのコンテンツキー $K_c(s)$ 、 $K_c(s+1 \bmod 32)$ を適用して各セクタ毎の暗号化処理を実行(S1609)する。

【0247】

セクタデータの復号処理の異なる処理態様を図46に示す。図46において、ステップS1701～S1708は、図45の各ステップS1601～S1608と同様である。ステップS1709～S1711が図45とは異なる。

【0248】

ステップS1705において、暗号化アルゴリズムがトリプルDESであると判定された場合、ステップS1709においてセクタNo. (s)を判定し、sが奇数である場合は、 $s = s - 1$ の更新を実行(S1710)し、各セクタに適用する鍵を $K_c(s)$ 、 $K_c(s+1)$ としてトリプルDESによる復号処理(S1711)を実行する。

【0249】

図42に戻り、ファイルの暗号化書き込み処理フローの説明を続ける。上述の処理によってデータ部の暗号化処理ステップ(S1334)が終了すると、データ部に対する誤り訂正符号を生成(S1335)し、暗号化されたデータ $D(i)$ とセクタデータに対応する改竄チェック値ICVと、誤り訂正符号を持つ冗長

部をメディアに書き込み（S1336）、書き込み成功フラグを1（成功）にセット（S1337）し、ビジーフラグを0（待機）に設定（S1339）する。

【0250】

なお、書き込み対象データがBPTによる管理のなされていない内部メモリ内への書き込み処理である場合は、ステップS1329、S1330はスキップする。ステップS1329、S1330の判定がNoである場合、すなわちメディアのセットフラグが1でない場合、または、BPTにセクタS(i)の書き込み許可が設定されていない場合には、ステップS1338に進み、書き込みエラーとして書き込み成功フラグを0にセットする。

【0251】

また、制御部は、ステップS1341～S1345において、メモリインタフェースのステータスを読み出して、ビジーフラグが0の状態において、書き込み成功フラグが1であることを条件としてアドレスを順次インクリメントして、書き込みデータを順次メモリインタフェースに送信する。すべての処理が終了すると、ファイル割り当てテーブルの更新処理を実行（S1346）し、更新したファイル割り当てテーブルを更新コマンドとともにメモリインタフェースに送信（S1347）し、メモリインタフェースはコマンドに従ってファイル割り当てテーブルの書き込み処理を実行（S1340）する。

【0252】

以上の、図41～図46によって説明した処理により、データの暗号化、メディアに対する格納処理が実行される。

【0253】

〔リボケーションリストの更新〕

次に、不正なメディアやコンテンツの失効情報としてのリボケーションリストの更新処理について説明する。前述したように、本発明におけるリボケーションリストは、複数の種類（ex. メディア、コンテンツ）の識別子（ID）から構成される。コンテンツやメディアの失効情報であるリボケーションリスト（Revocation List）に複数の種類のIDを設け、それぞれの照合を異なる動作として行うことによって、1つのリボケーションリストで複数の種類のコンテンツ、メ

メディアを排除することが可能となる。メディアの挿入時やコンテンツの読み出し時にメモリ・インターフェース部において、利用メディアまたは利用コンテンツの識別子（ID）と、リボケーションリストのリスティングIDとの照合を実行することにより、不正なメディアの使用や不正なコンテンツの読み出しを禁止することができる。

【0254】

先に説明したように、リボケーションリストには、リボケーションリストバージョン（Revocation List Version）が設定され、新たな不正なメディアやコンテンツの失効情報を追加した場合等にリボケーションリストは更新される。

【0255】

リボケーションリストの更新処理フローを図47に示す。図47において、左側はデバイスの制御部、右側はデバイスのメモリインタフェースである。

【0256】

まず、制御部は更新用のリボケーションリストを通信部201（図2参照）から受信する（S1801）と、更新用リボケーションリストチェックコマンドと、受信した更新用リボケーションリストをメモリインタフェースに送信（S1802）する。

【0257】

メモリインタフェースは、更新用リボケーションリストチェックコマンドと、更新用リボケーションリストを制御部から受信（S1803）すると、ビジーフラグを1（ビジー）に設定（S1804）し、リボケーションリストの改竄チェック値（ICV）生成鍵Kicv_rlを生成（S1805）する。

【0258】

リボケーションリストの改竄チェック用の改竄チェック値（ICV）生成鍵Kicv_rlは、予めデバイス内に格納されたりボケーションリスト（Revocation List）のICV鍵を生成するマスター鍵：MKicv_rlと、リボケーションリスト（Revocation List）のICV鍵を生成する時の初期値：IVicv_rlと、リボケーションリストの属性情報中に含まれるリボケーションリスト・バージョン（Version）に基づいて生成する。具体的には、改竄チェック値（ICV）生成鍵

$Kicv_rl = DES(E, MKicv_rl, Version \cdot IVicv_rl)$ に基づいて改竄チェック値 (ICV) 生成鍵が生成される。前記式の意味は、バージョン (Version) と初期値 (IVicv_rl) の排他論理和にマスター鍵: MKicv_rl による DES モードでの暗号化処理を実行するという意味である。

【0259】

次にメモリアンタフェースは生成した改竄チェック値 (ICV) 生成鍵 $Kicv_rl$ を用いてリボケーションリストの ICV' を生成 (S1806) し、予めリボケーションリスト内に格納された正しい ICV 値と照合 $ICV' = ICV ?$ を実行 (S1807) する。なお、 ICV' の生成処理は、前述の図 14 で説明した DES モードに基づいて、初期値 $IVrl$ を用い、生成した改竄チェック値 (ICV) 生成鍵 $Kicv_rl$ を適用した処理によって行われる。

【0260】

$ICV' = ICV$ である場合 (S1807 で Yes) は、更新用リボケーションリストが改竄のない正当なものであると判定され、ステップ S1808 に進み、現在セットされているリボケーションリストのバージョン (i) と更新用リボケーションリストのバージョン (j) を比較 (S1809) し、更新用リボケーションリストのバージョンが新しい場合には、更新用リボケーションリストの有効フラグを 1 に設定 (S1810) し、ビジーフラグを 0 にセット (S1811) して処理を終了する。

【0261】

一方、制御部側は、ステータス読み出しコマンドをメモリアンタフェースに送信 (S1812) し、ビジーフラグが 0 となった (S1813) ことを確認し、更新用リボケーションリスト有効フラグが 1 (S1814) である場合に、更新用リボケーションリストを通常のファイルとして内部メモリに保存 (S1815) する。コンテンツの処理、メディアの装着時のチェックの際には、内部メモリに格納されたりボケーションリストが読み出される。

【0262】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得

ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0263】

【発明の効果】

以上、説明したように、本発明のデータ記憶装置、およびデータ記録方法、データ再生方法によれば、コンテンツのセクタ対応の暗号処理鍵について、データ記録再生装置とデータ記憶装置間におけるCBCモードでの暗号化を実行し、CBCモードで暗号化された鍵データをコンテンツに対応するヘッダに格納する構成としたので、暗号化された鍵データからの不正復号処理が困難となり、安全な鍵の保存が可能となる。

【0264】

さらに、本発明のデータ記憶装置、およびデータ記録方法、データ再生方法によれば、CBCモードによる鍵の暗号化処理をコンテンツを格納するメディアに固有の保存鍵を適用して行なう構成とし、例えばコンテンツ利用時には、相互認証の成立したメディアにおいて鍵データを復号することによってのみ鍵を取得可能としたので、デバイス単独、あるいは不正なメディアを装着した場合には鍵データの復号が不可能であり安全な鍵の保存が可能となる。

【図面の簡単な説明】

【図1】

本発明のデータ処理装置の使用概念を説明する図である。

【図2】

本発明のデータ処理装置のデバイスおよびメディアの構成を示す図である。

【図3】

本発明のデータ処理装置のメモリ格納データ構成を示す図である。

【図4】

本発明のデータ処理装置にデバイスのメモリインタフェースの詳細構成を示す図である。

【図5】

本発明のデータ処理装置におけるメモリインタフェースのステータスレジスタのデータ構成を示す図である。

【図 6】

本発明のデータ処理装置におけるメディアに格納されるデータの詳細構成を示す図である。

【図 7】

本発明のデータ処理装置においてメディアに格納されるコンテンツに対応して設定されるセキュリティヘッダの構成を説明する図である。

【図 8】

本発明のデータ処理装置におけるデータ暗号化の 2 つの態様を説明する図である。

【図 9】

本発明のデータ処理装置におけるリボケーションリストの構成を示す図である。

【図 1 0】

本発明のデータ処理装置におけるブロック・パーミッション・テーブル（B P T）について説明する図である。

【図 1 1】

本発明のデータ処理装置におけるメディア 1 製造時の B P T 格納処理フローを示す図である。

【図 1 2】

本発明のデータ処理装置におけるメディア 2 製造時の B P T 格納処理フローを示す図である。

【図 1 3】

本発明のデータ処理装置におけるブロック・パーミッション・テーブル（B P T）の具体例について説明する図である。

【図 1 4】

本発明のデータ処理装置における改竄チェック値生成処理構成について説明する図である。

【図 1 5】

本発明のデータ処理装置における改竄チェック値検証処理フローについて説明する図である。

【図 1 6】

本発明のデータ処理装置におけるデバイス起動時フローを示す図である。

【図 1 7】

本発明のデータ処理装置におけるファイル割り当てテーブルの構成例について説明する図である。

【図 1 8】

本発明のデータ処理装置におけるメディア 1 認識時フロー（その 1）を示す図である。

【図 1 9】

本発明のデータ処理装置におけるメディア 1 認識時フロー（その 2）を示す図である。

【図 2 0】

本発明のデータ処理装置におけるメディア 2 認識時フロー（その 1）を示す図である。

【図 2 1】

本発明のデータ処理装置におけるメディア 2 認識時フロー（その 2）を示す図である。

【図 2 2】

本発明のデータ処理装置においてデバイス・メディア間において実行される相互認証処理シーケンスを示す図である。

【図 2 3】

本発明のデータ処理装置における相互認証・鍵共有処理フロー（その 1）を示す図である。

【図 2 4】

本発明のデータ処理装置における相互認証・鍵共有処理フロー（その 2）を示す図である。

【図 2 5】

本発明のデータ処理装置におけるファイルの読み出し処理フローを示す図である。

【図 2 6】

本発明のデータ処理装置におけるファイルの書き込み処理フローを示す図である。

【図 2 7】

本発明のデータ処理装置におけるメモリに格納されたデータの暗号化処理態様を説明する図である。

【図 2 8】

本発明のデータ処理装置におけるメモリに格納されたデータの暗号化処理態様として適用可能なトリプル D E S を説明する図である。

【図 2 9】

本発明のデータ処理装置におけるメモリに格納されたデータの暗号化処理態様を説明する図である。

【図 3 0】

本発明のデータ処理装置におけるメモリに格納されたデータの暗号化処理態様を説明する図である。

【図 3 1】

本発明のデータ処理装置におけるセクタ対応改竄チェック値の格納処理態様を説明する図である。

【図 3 2】

本発明のデータ処理装置におけるセクタ対応コンテンツキー他の鍵の暗号化処理例を説明する図である。

【図 3 3】

本発明のデータ処理装置におけるセクタ対応コンテンツキー他の鍵の復号処理例を説明する図である。

【図 3 4】

本発明のデータ処理装置におけるセクタ対応コンテンツキー他の鍵のデバイス

・メディア間における処理例を説明する図である。

【図 3 5】

本発明のデータ処理装置におけるファイルの復号読み出し処理フロー（その 1）を示す図である。

【図 3 6】

本発明のデータ処理装置におけるファイルの復号読み出し処理フロー（その 2）を示す図である。

【図 3 7】

本発明のデータ処理装置におけるコンテンツキー他の復号処理フローを示す図である。

【図 3 8】

本発明のデータ処理装置におけるコンテンツキー他のメディアの保存鍵による復号処理フローを示す図である。

【図 3 9】

本発明のデータ処理装置におけるセクタデータの復号処理フロー（その 1）を示す図である。

【図 4 0】

本発明のデータ処理装置におけるセクタデータの復号処理フロー（その 2）を示す図である。

【図 4 1】

本発明のデータ処理装置におけるファイルの暗号化書き込み処理フロー（その 1）を示す図である。

【図 4 2】

本発明のデータ処理装置におけるファイルの暗号化書き込み処理フロー（その 2）を示す図である。

【図 4 3】

本発明のデータ処理装置におけるコンテンツキー他の暗号化処理フローを示す図である。

【図 4 4】

本発明のデータ処理装置におけるコンテンツキー他のメディアの保存鍵による暗号化処理フローを示す図である。

【図 4 5】

本発明のデータ処理装置におけるセクタデータの暗号化処理フロー（その 1）を示す図である。

【図 4 6】

本発明のデータ処理装置におけるセクタデータの暗号化処理フロー（その 2）を示す図である。

【図 4 7】

本発明のデータ処理装置におけるリボケーションリストの更新処理フローを示す図である。

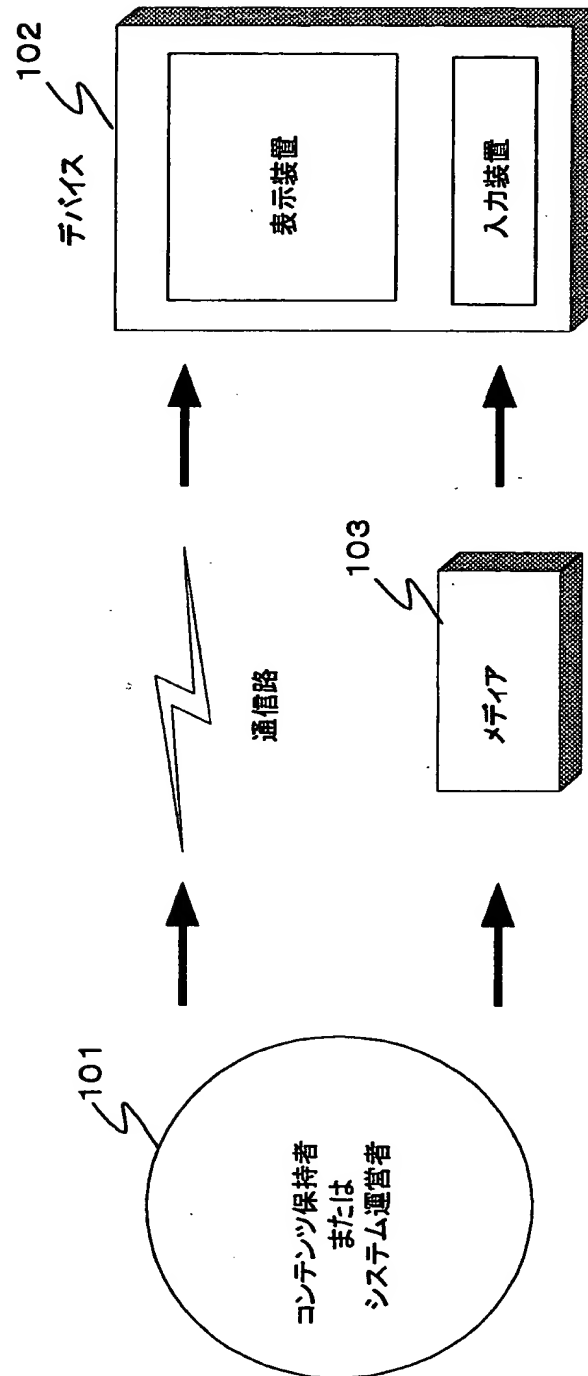
【符号の説明】

- 1 0 1 システム運営者
- 1 0 2 デバイス
- 1 0 3 メディア
- 2 0 0 デバイス
- 2 0 1 通信部
- 2 0 2 入力部
- 2 0 3 表示部
- 2 0 4 デバイスコントローラ
- 2 0 5 制御部
- 2 0 7 メモリ部
- 3 0 0 メモリインタフェース（I/F）部
- 2 1 0 メディア 1
- 2 1 1 制御部
- 2 1 2 メモリ部
- 2 3 0 メディア 2
- 2 3 1 コントローラ
- 2 3 2 メモリ部

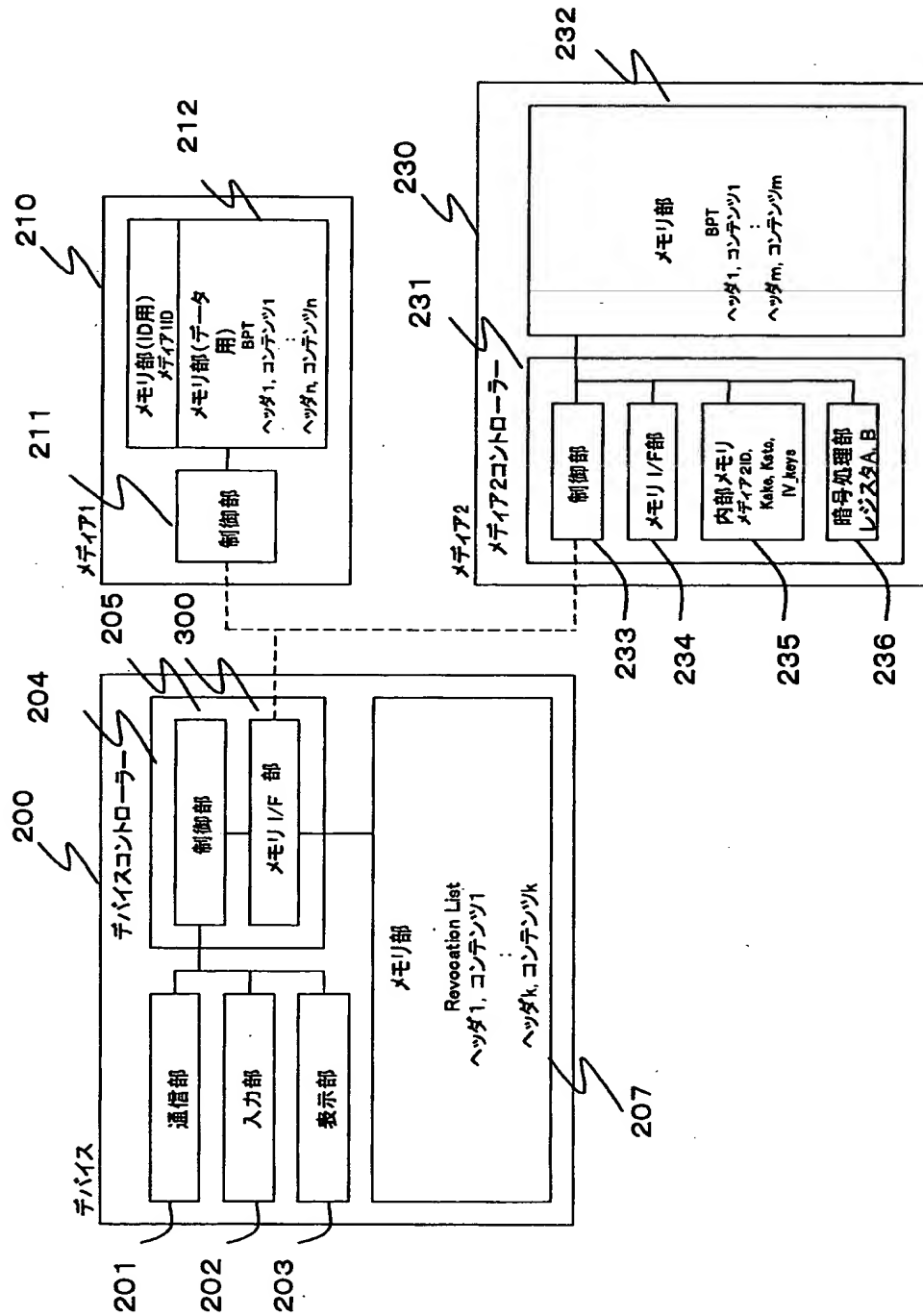
- 2 3 3 制御部
- 2 3 4 メモリインタフェース (I / F) 部
- 2 3 5 内部メモリ
- 2 3 6 暗号処理部
- 3 0 1 ステータスレジスタ
- 3 0 2 コマンドレジスタ
- 3 0 3 アドレスレジスタ
- 3 0 4 カウントレジスタ
- 3 0 5 コントロールレジスタ
- 3 0 6 送受信制御部
- 3 0 7 送信バッファメモリ
- 3 0 8 受信バッファメモリ
- 3 0 9 送信レジスタ
- 3 1 0 受信レジスタ
- 3 2 0 暗号処理部
- 3 2 1 メモリ部
- 3 2 3 E C C 回路
- 3 2 4 外部メモリ入出力インタフェース
- 3 2 5 内部メモリ入出力インタフェース

【書類名】 図面

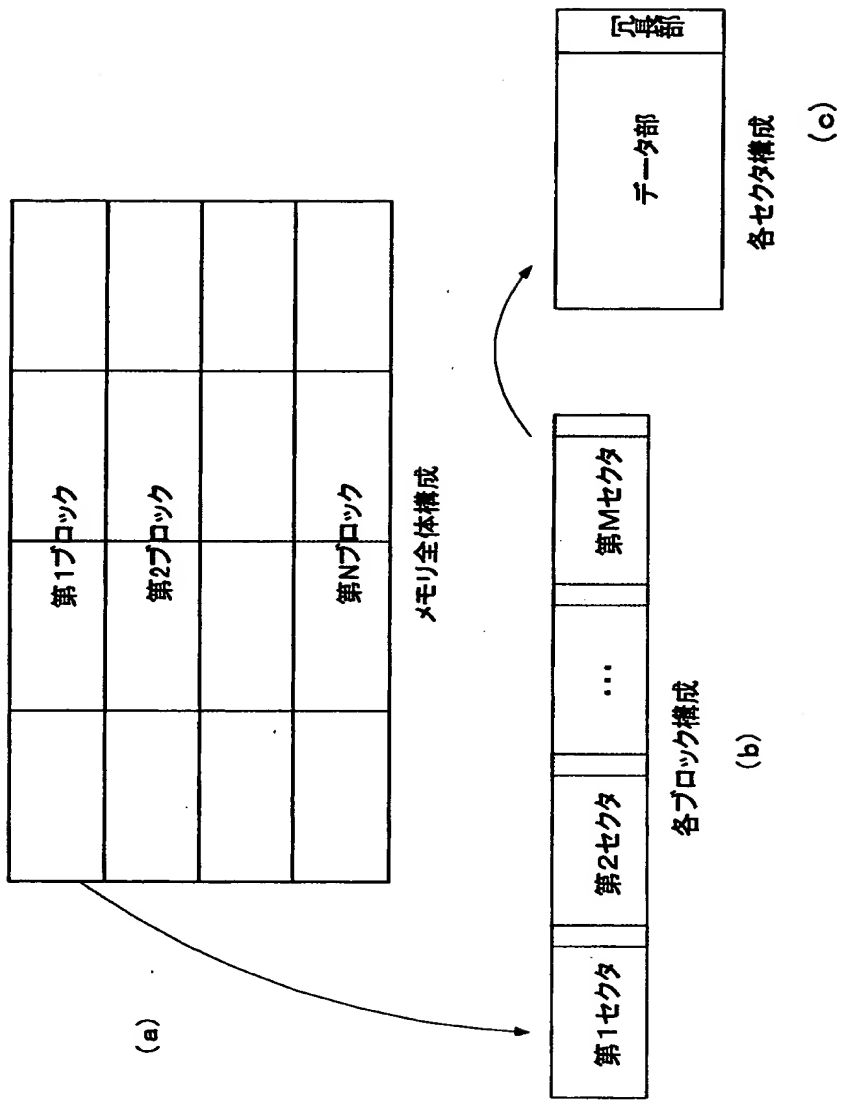
【図 1】



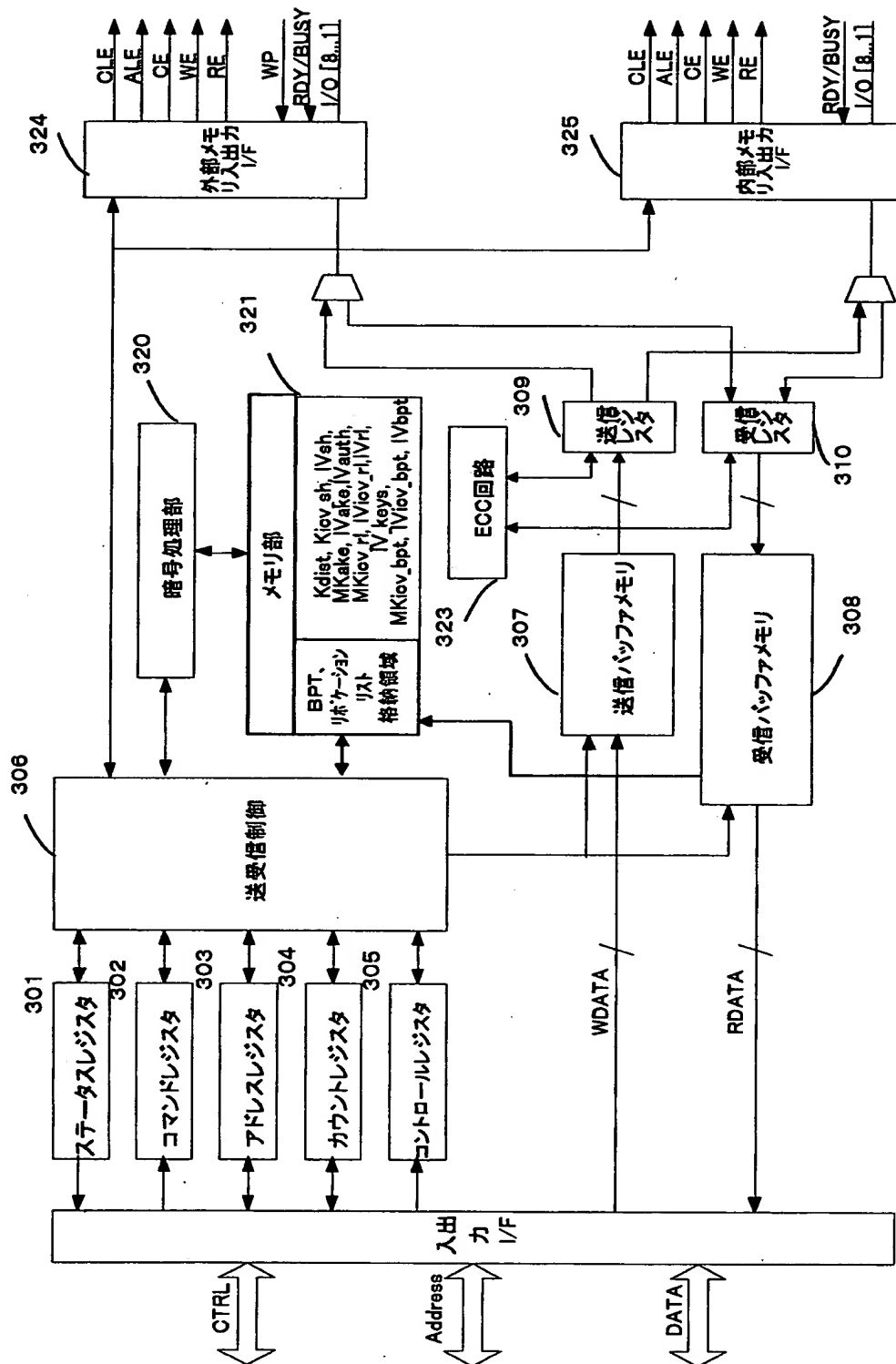
【図2】



【図3】



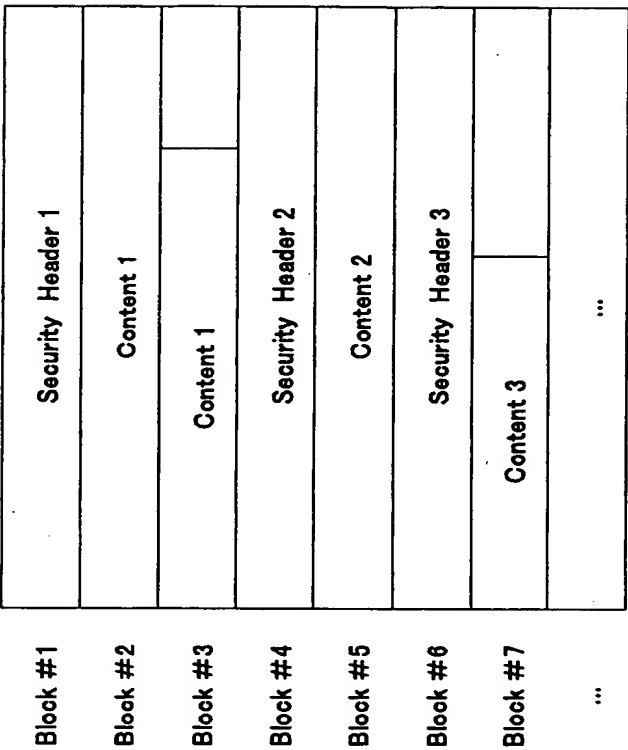
【図 4】



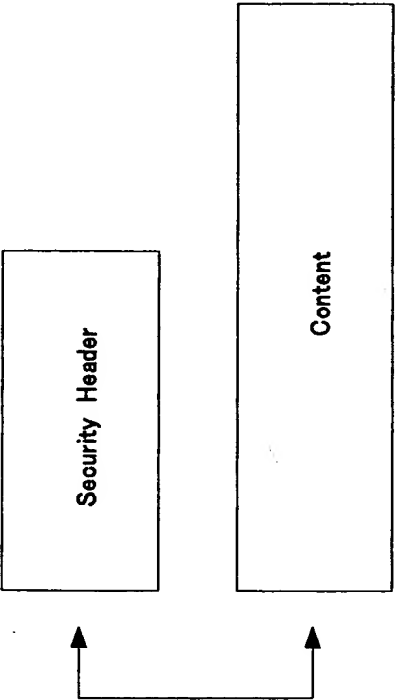
【図 5】

bit 10	bit 9	bit 8	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
更新用Revocation List有効フラグ	Revocation List セットフラグ	ヘッダ生成 成功フラグ	ヘッダセッ ト 成功フラグ	メディア2 有効フラグ	メディア1 有効フラグ	メディア2 セットフラ グ	メディア1 セットフラ グ	書き込み成功 フラグ	読み出し成 功 フラグ	ビジーフラ グ

【図 6】



(b)

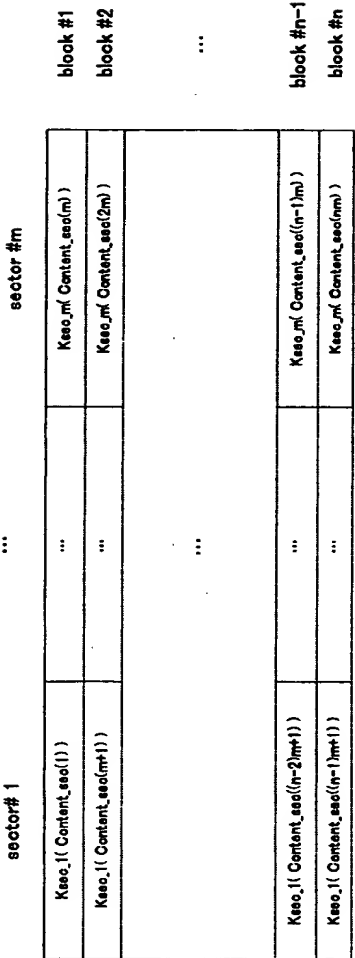
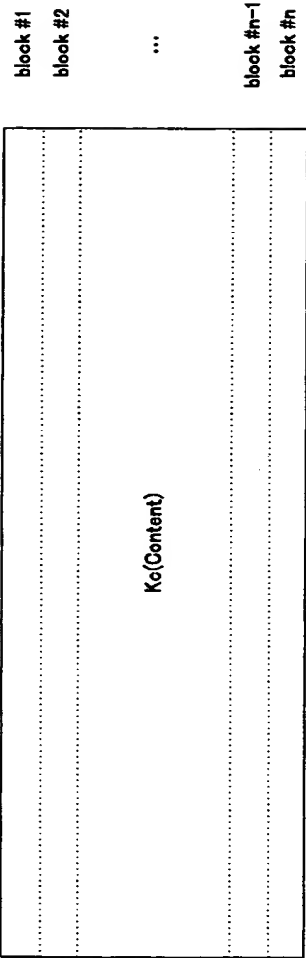


(a)

【図 7】

Format Version
Content ID
Content Type
Data Type
Encryption Algorithm
Encryption Mode
Encryption Format Type
Encryption Flag
ICV Flag
K ₀ _Encrypted 0
...
K ₀ _Encrypted 31
K _{icv} _cont_encrypted
Valid Revocation List version
ICV of Security Header

【図 8】



各ブロックのセクタ#1は
Kseo_1 で暗号化

↑

各ブロックのセクタ#mは
Kseo_m で暗号化

↑

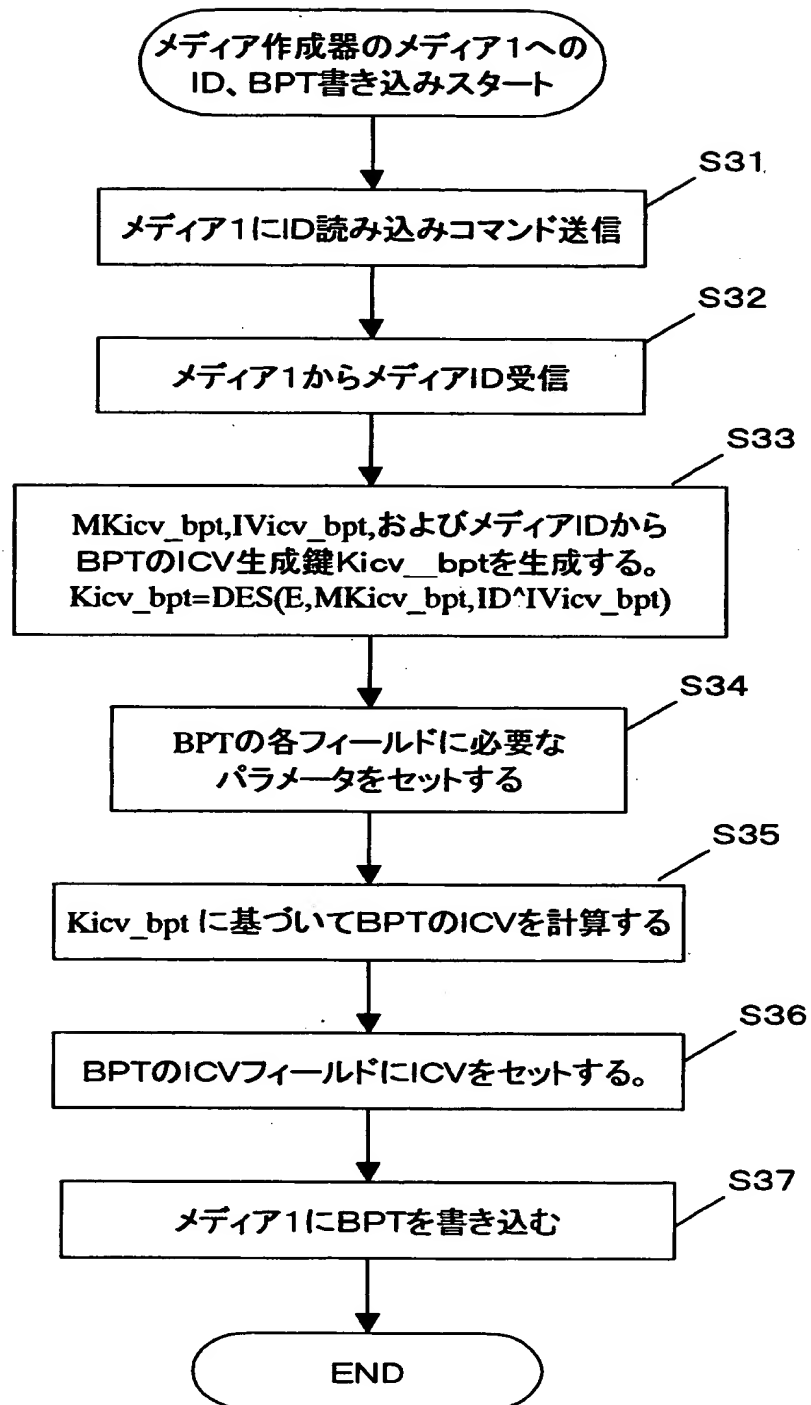
【図 9】

Revocation List ID
Revocation List Version
Number of Media1 ID
Media1 ID(0)
.....
Media1 ID(L-1)
Number of Media2 ID
Media2 ID(0)
.....
Media2 ID(M-1)
Number of Contents ID
Contents ID(0)
.....
Contents ID(N-1)
ICV of Revocation List

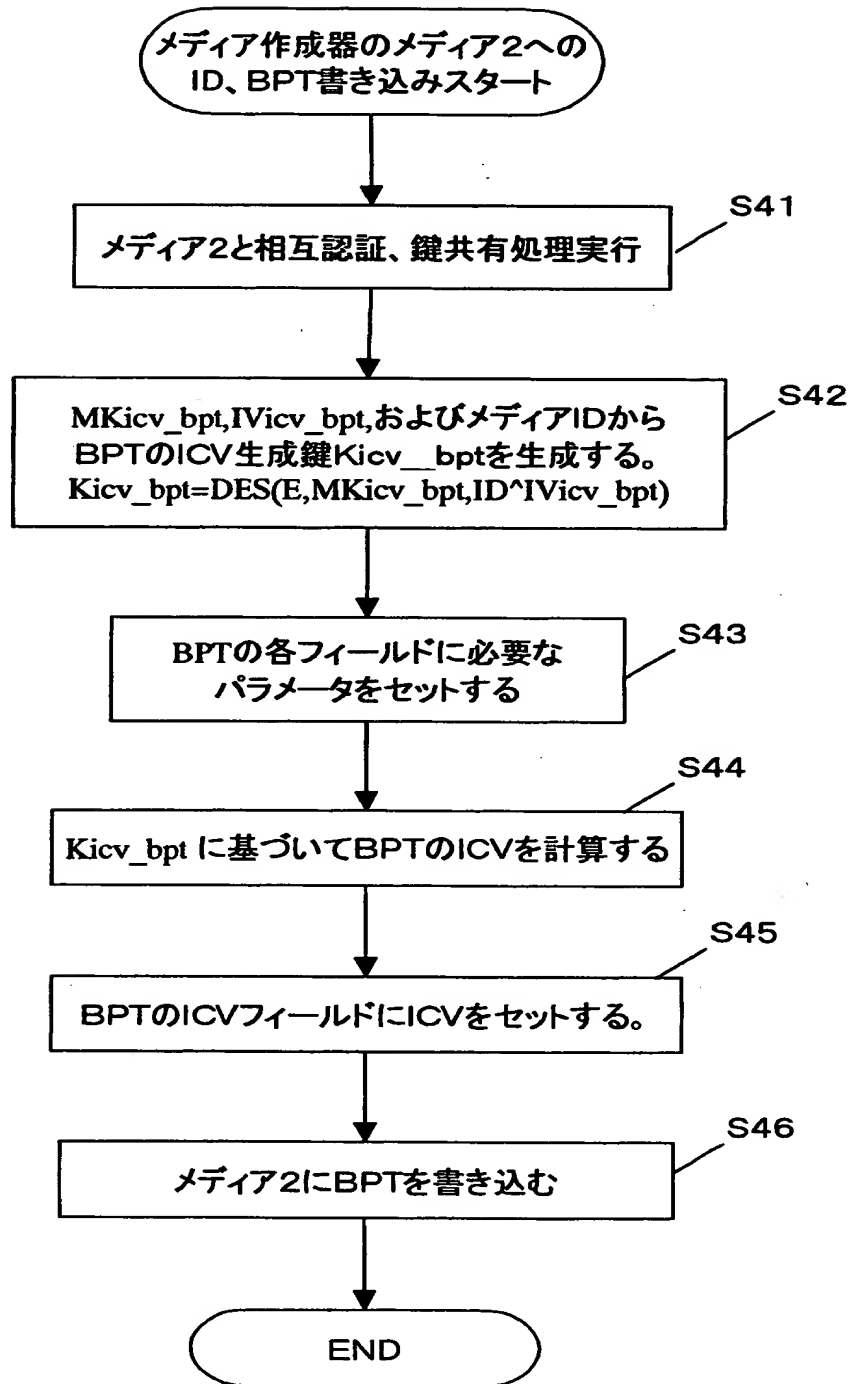
【図 1 0】

Format Version
BPT ID
Number of Blocks
Block #1 Permission Flag
...
Block #n Permission Flag
ICV of BPT

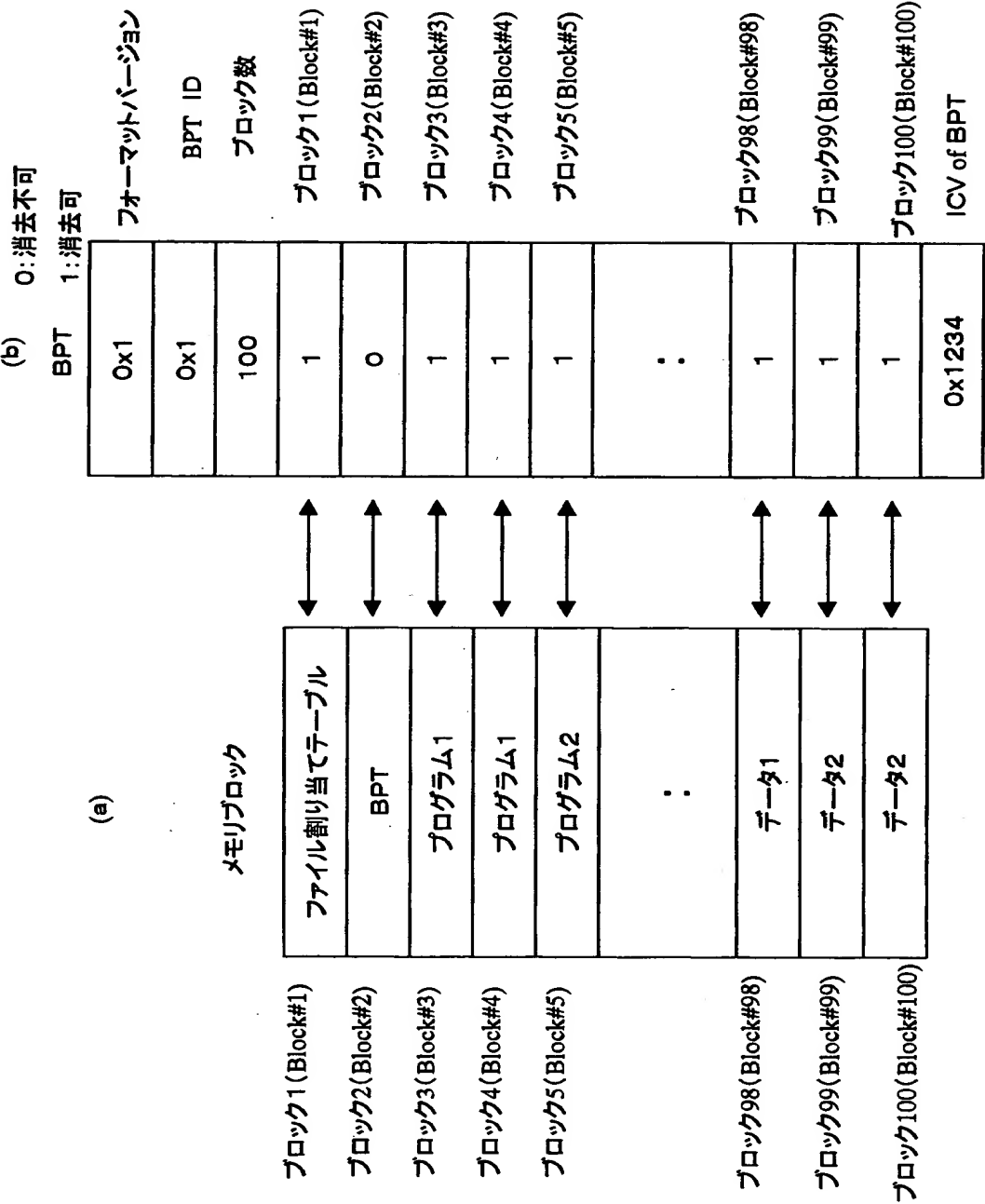
【図 11】



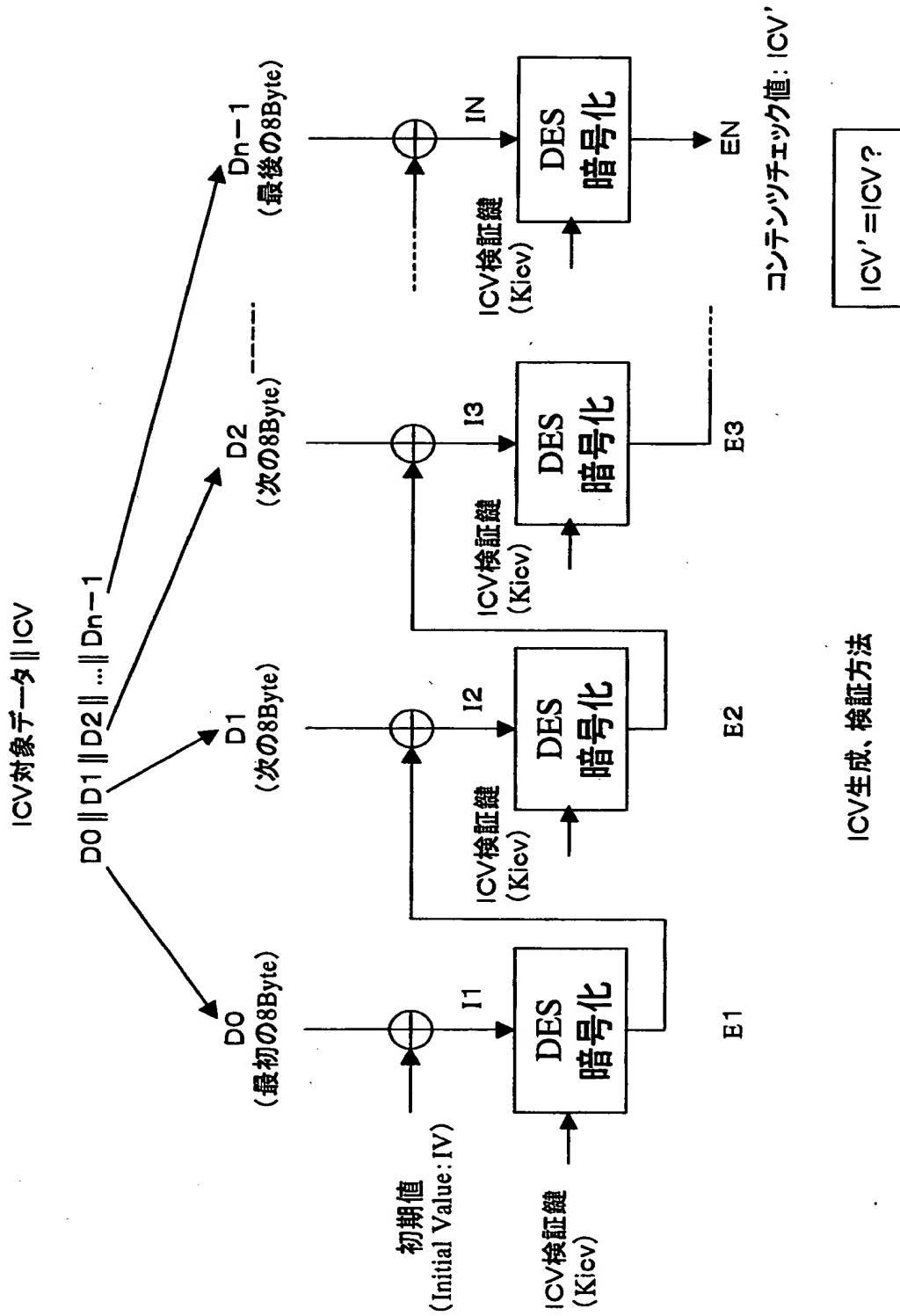
【図 12】



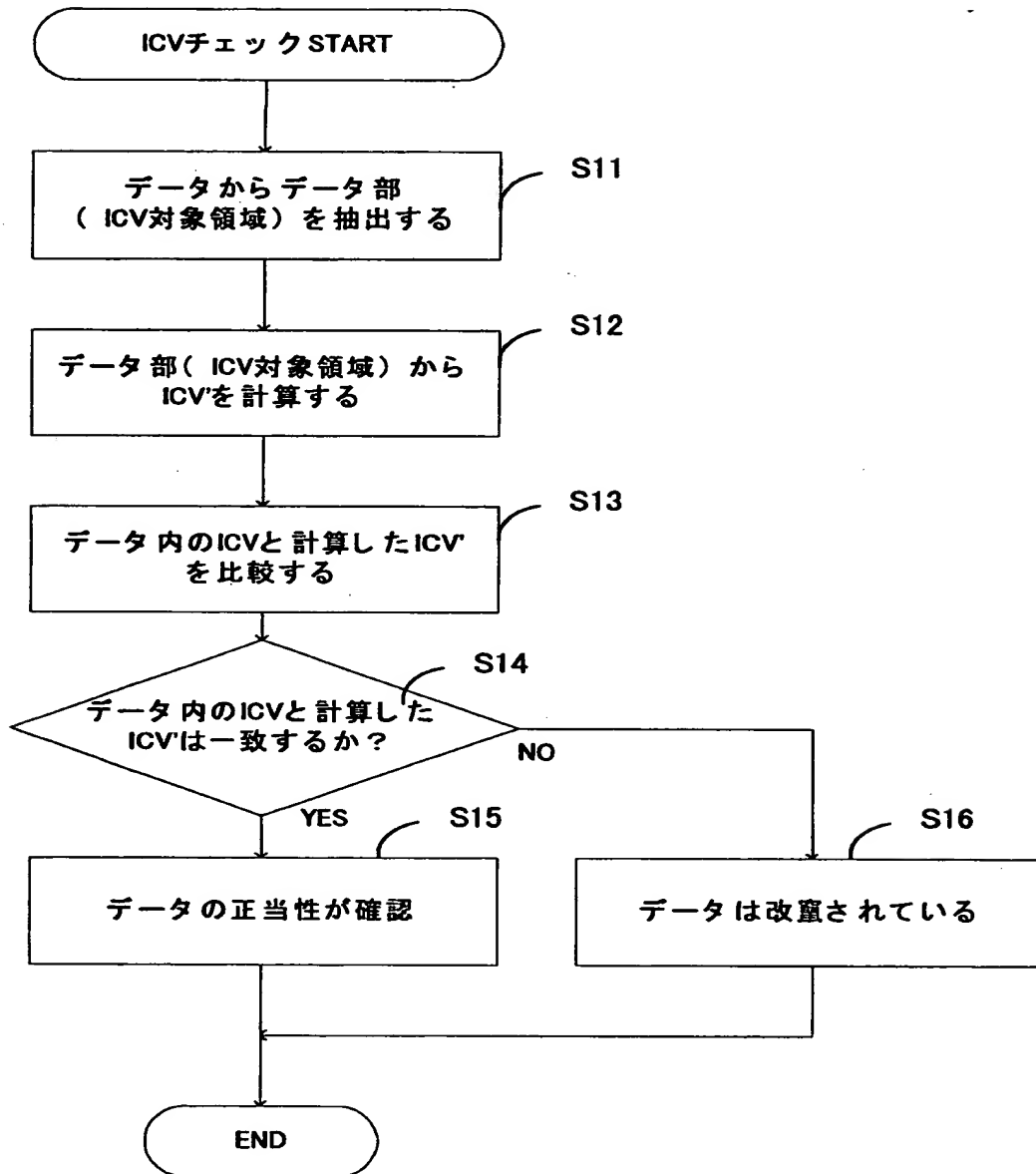
【図 1 3】



【図 1.4】

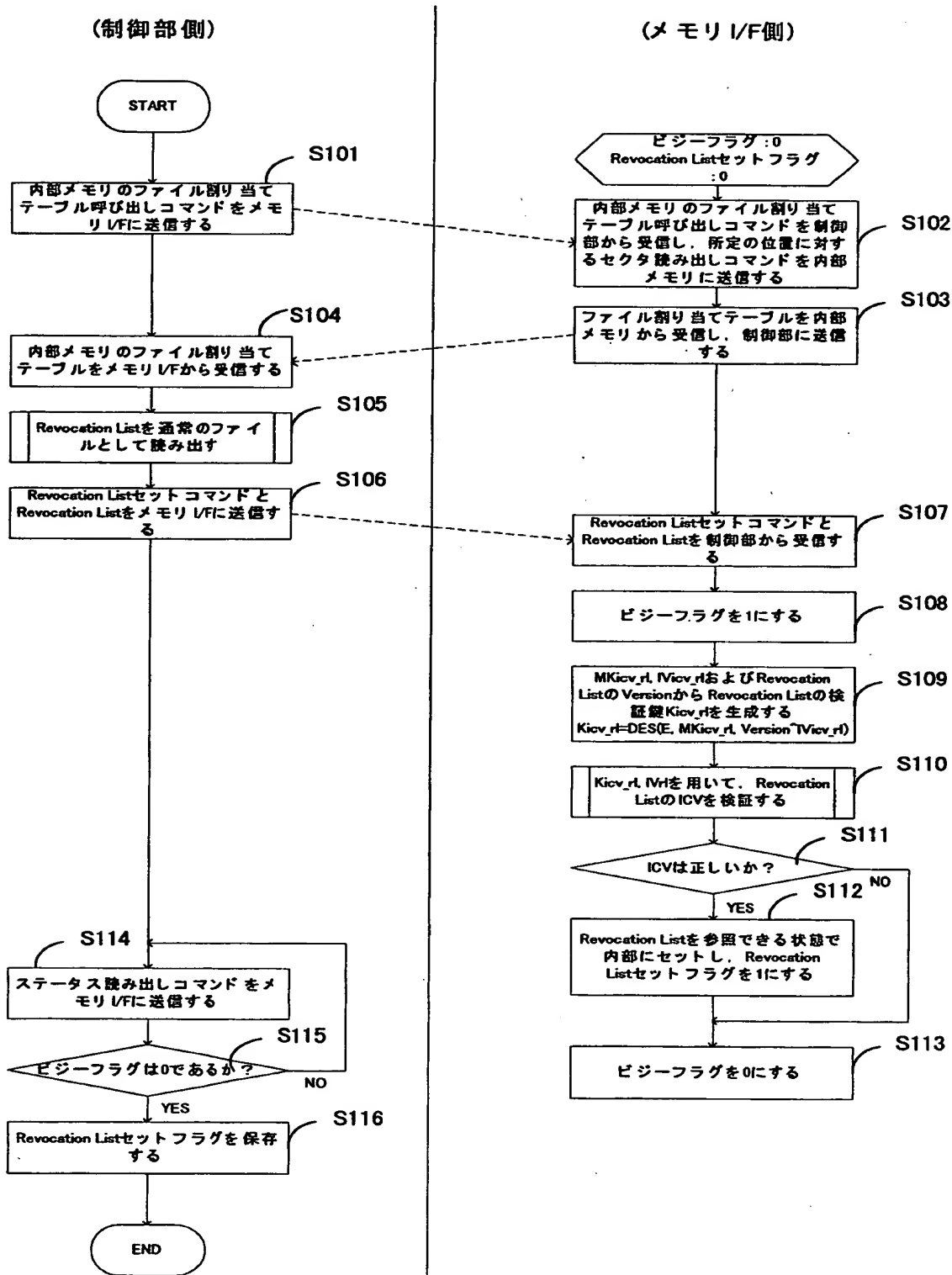


【図15】



ICVチェック

【図16】

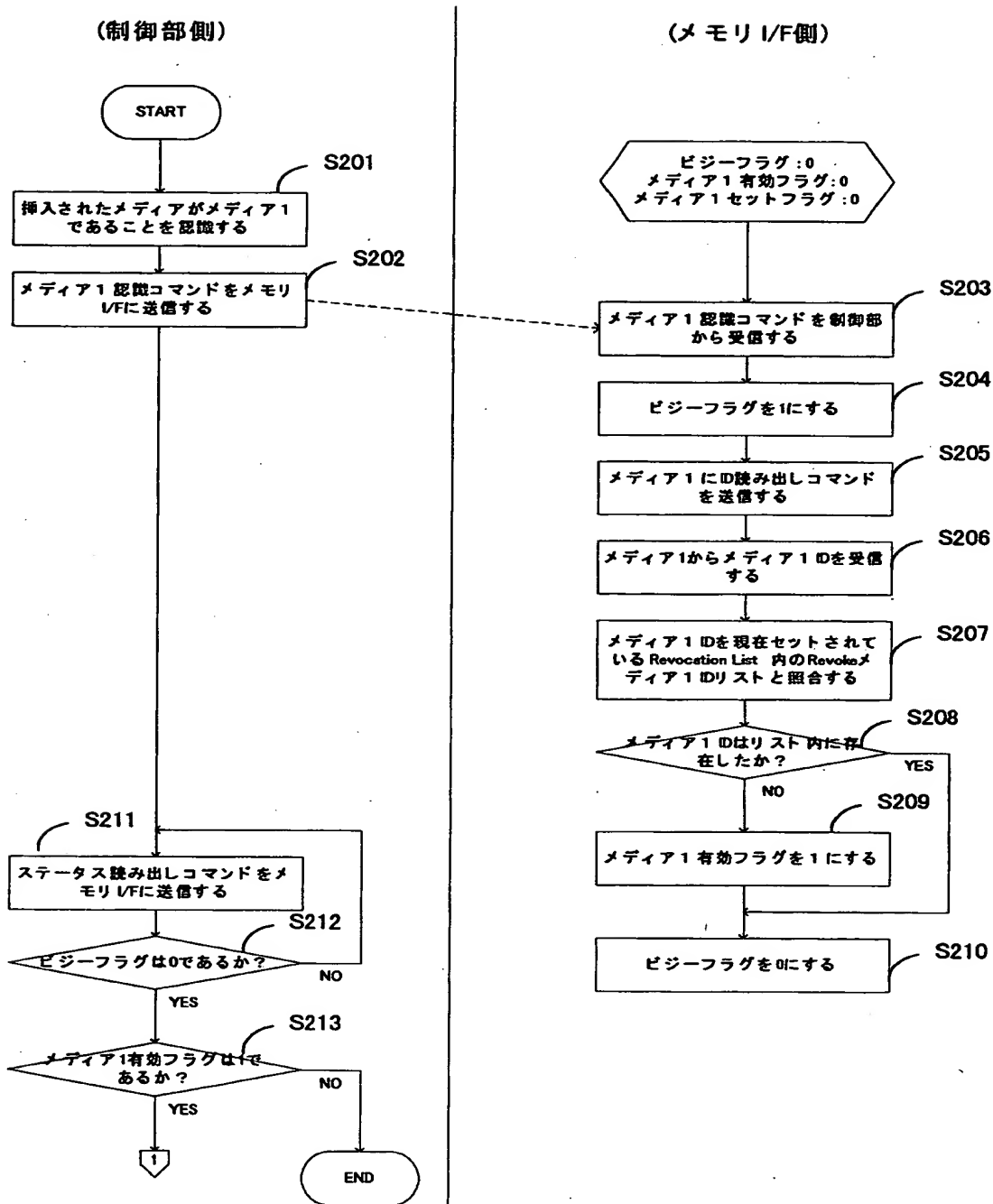


デバイス起動時フロー

【図17】

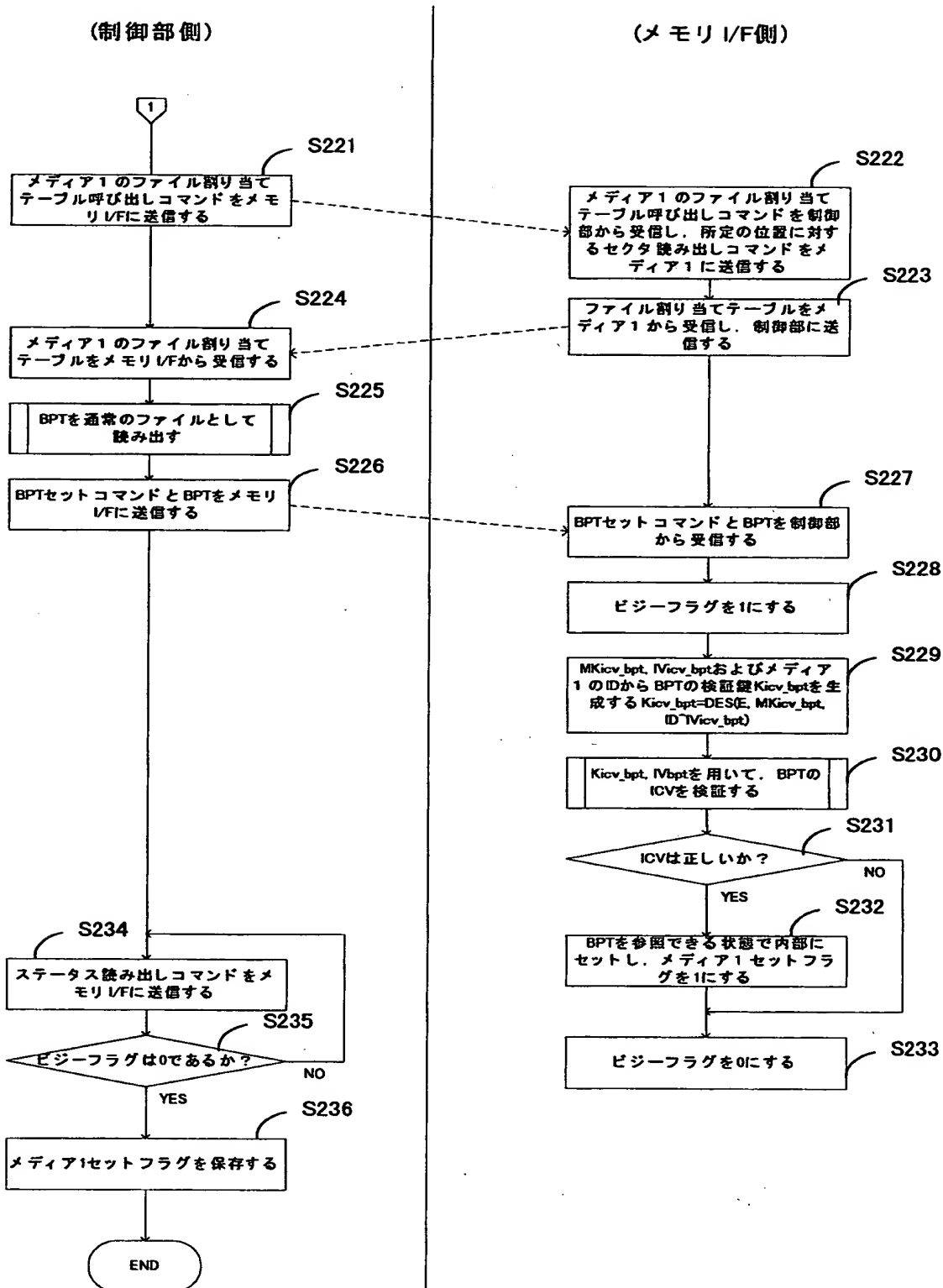
ディレクトリ	ファイル名	格納セクタ
/	A.h	1 ~ 10
/	A.cont	21 ~ 100
/dir_a	B.h	101 ~ 110
/dir_a	B.cont	111 ~ 350
/dir_a/dir_x	C	401 ~ 450
/dir_b	D	501 ~ 580
/dir_o	E.h	601 ~ 610
:	:	:
/dir_o	Z.cont	5001 ~ 5340

【図18】

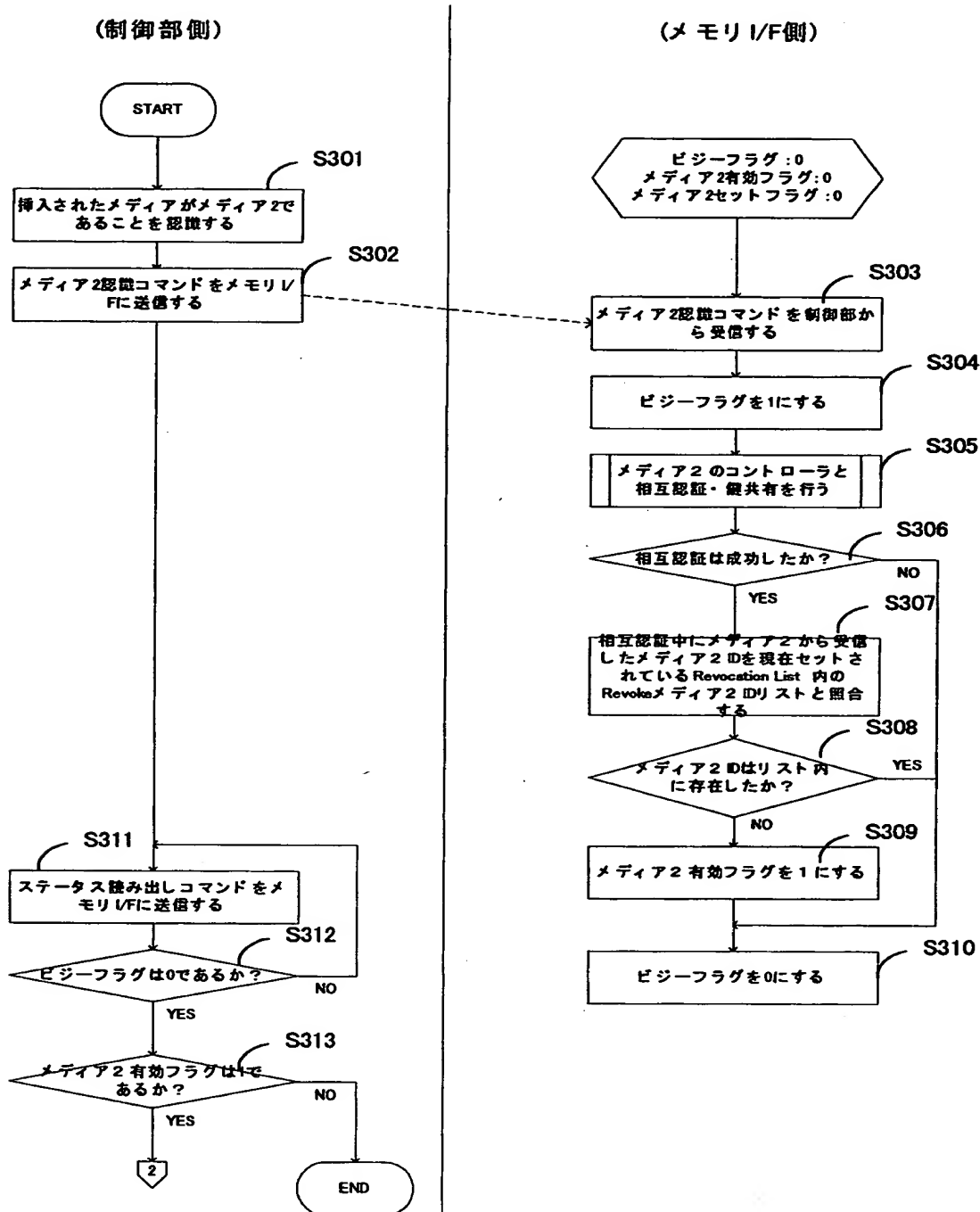


メディア1 認識時フロー

【図19】

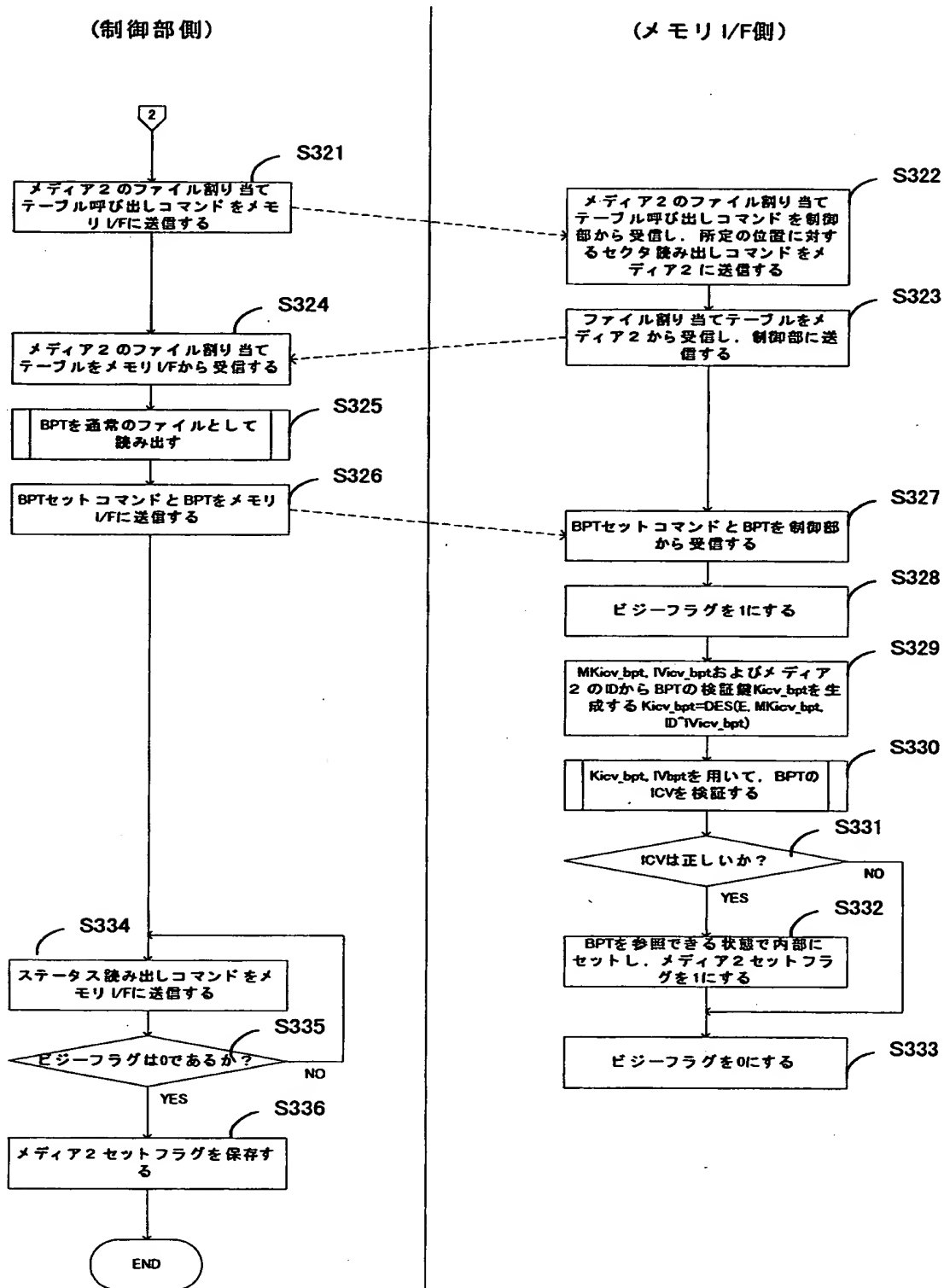


【図20】



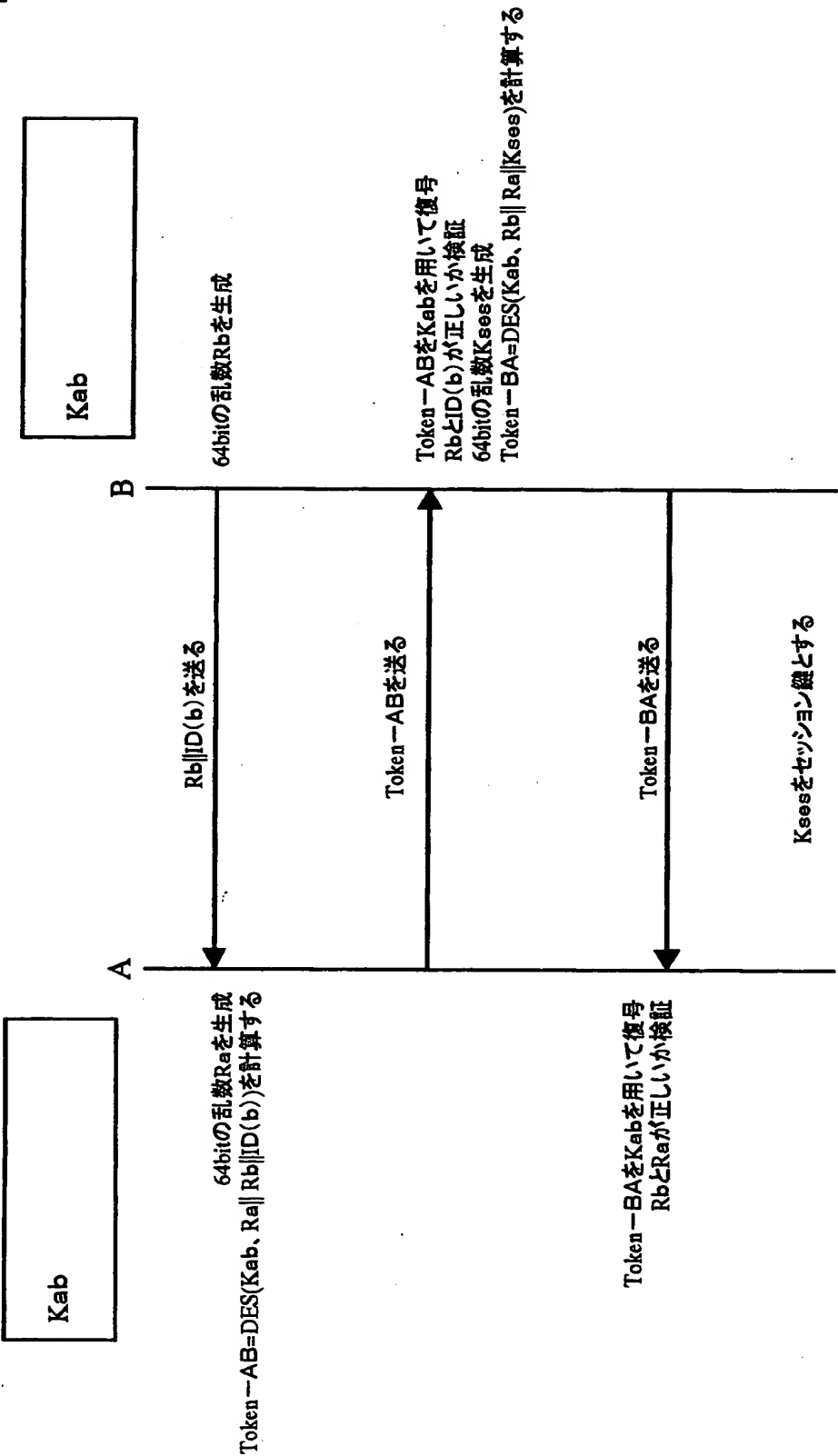
メディア2 認識時フロー

【図 21】



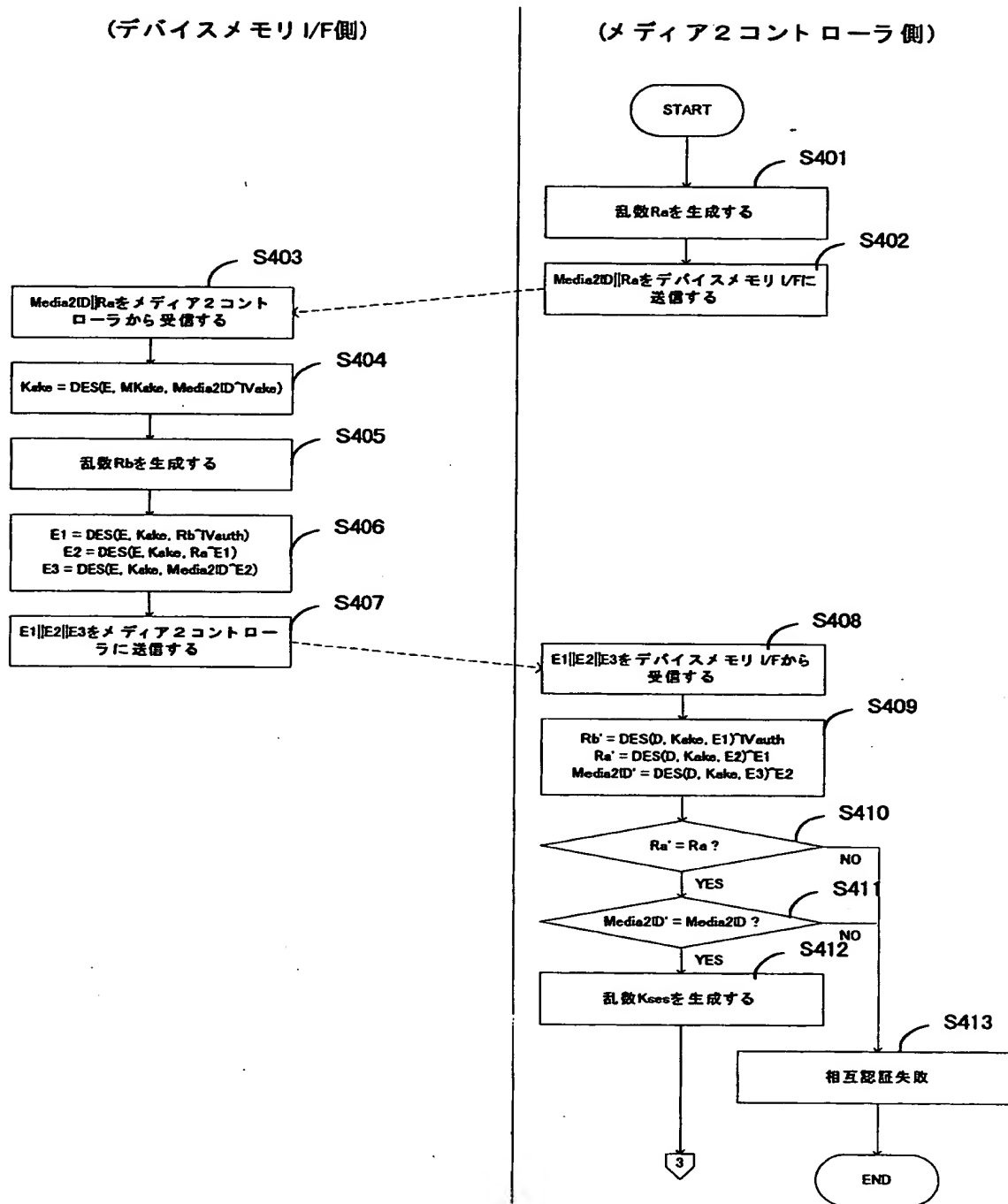
メディア2 認識時フロー（cont.）

【図 2 2】



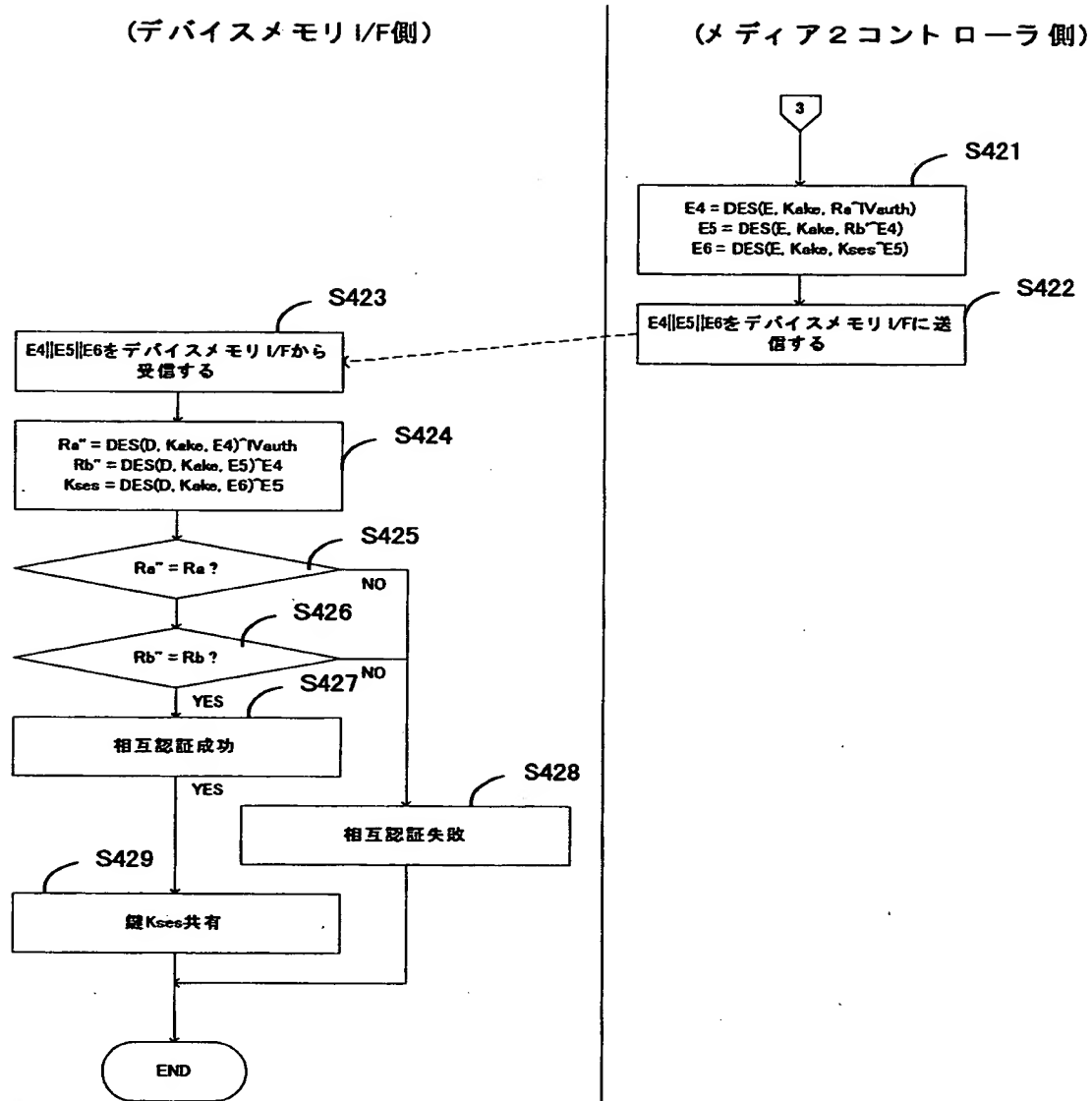
ISO/IEC 9798-2 対称鍵暗号技術を用いた相互認証および鍵共有方式

【図 23】



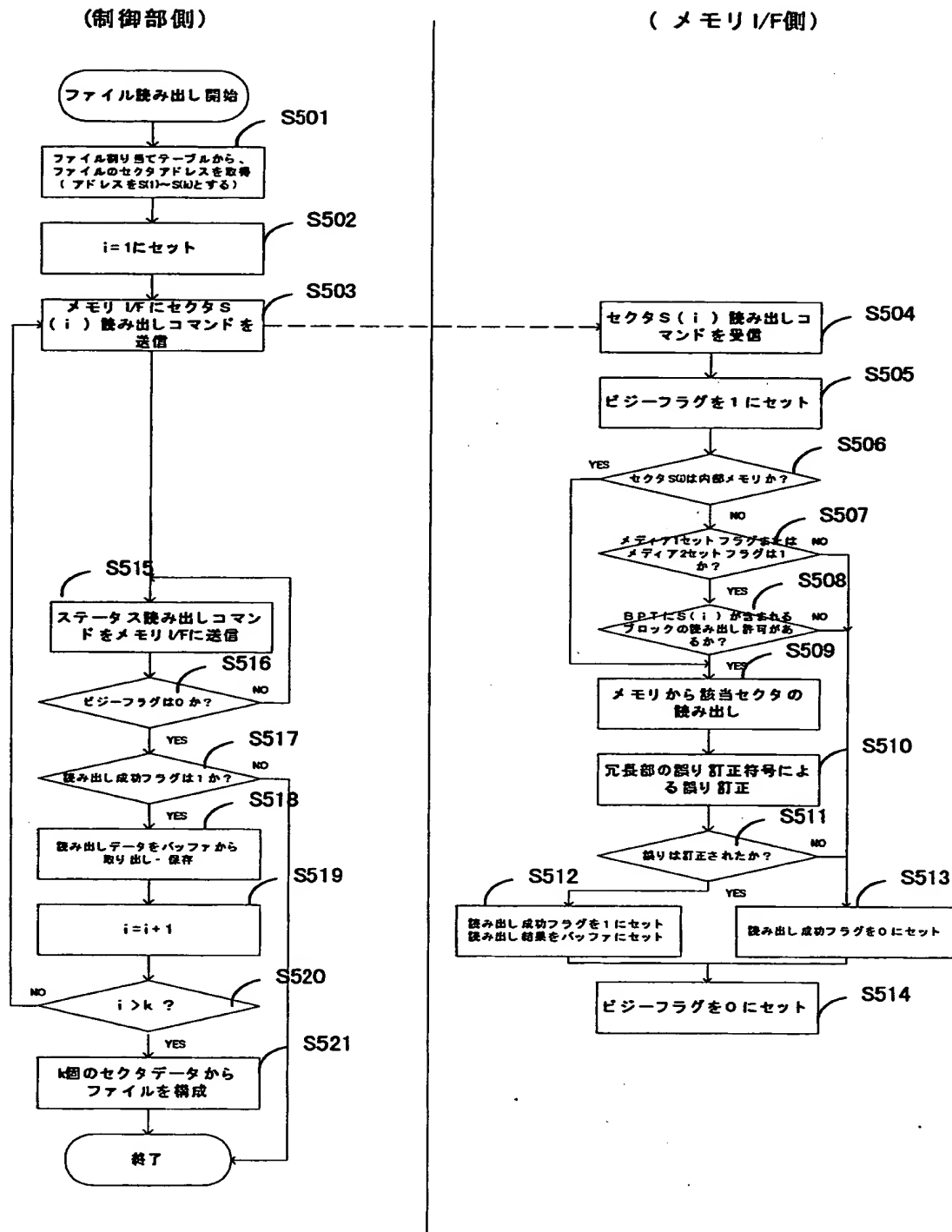
相互認証・鍵共有フロー

【図 24】

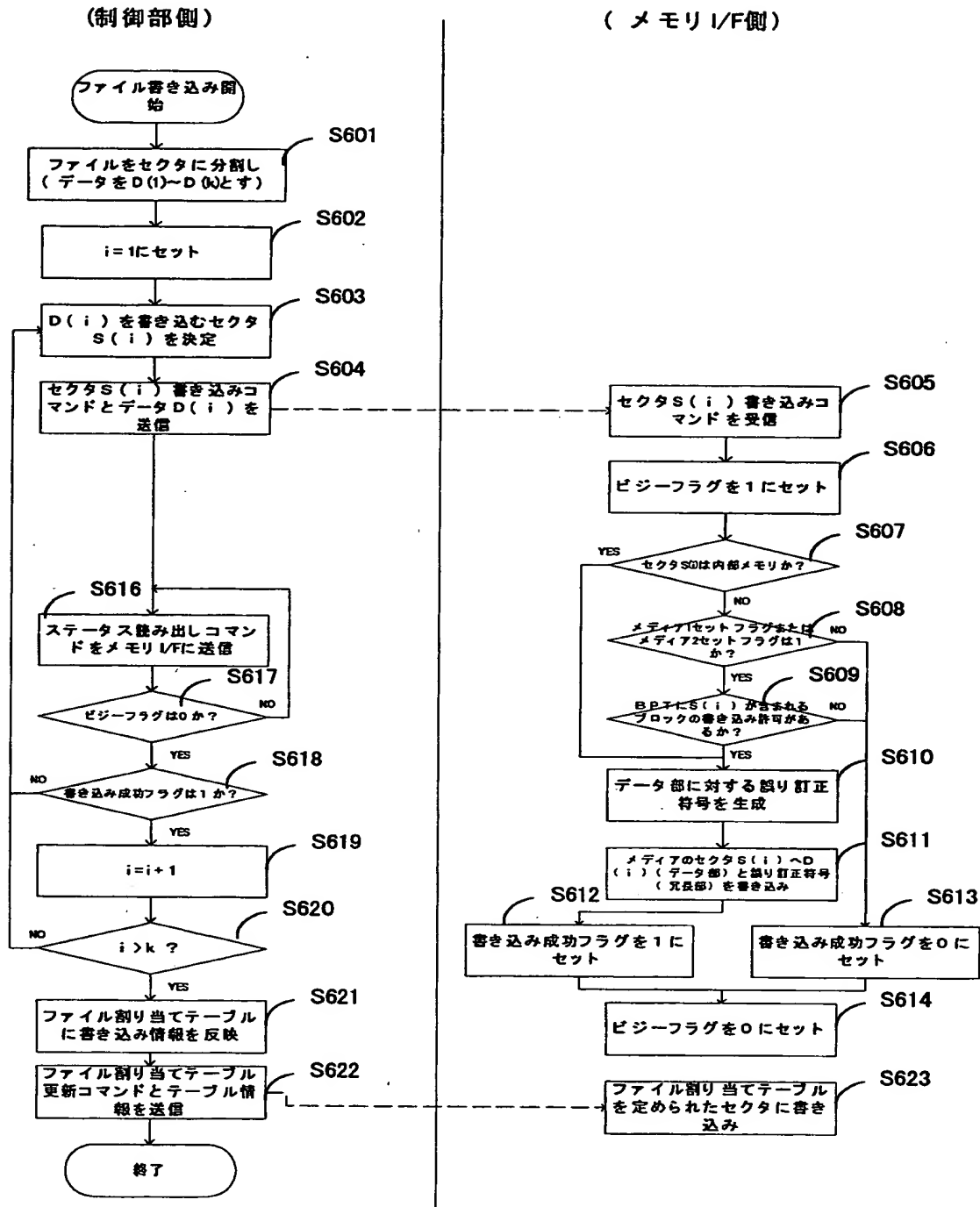


フロー 1-4: 相互認証・鍵共有フロー (cont.)

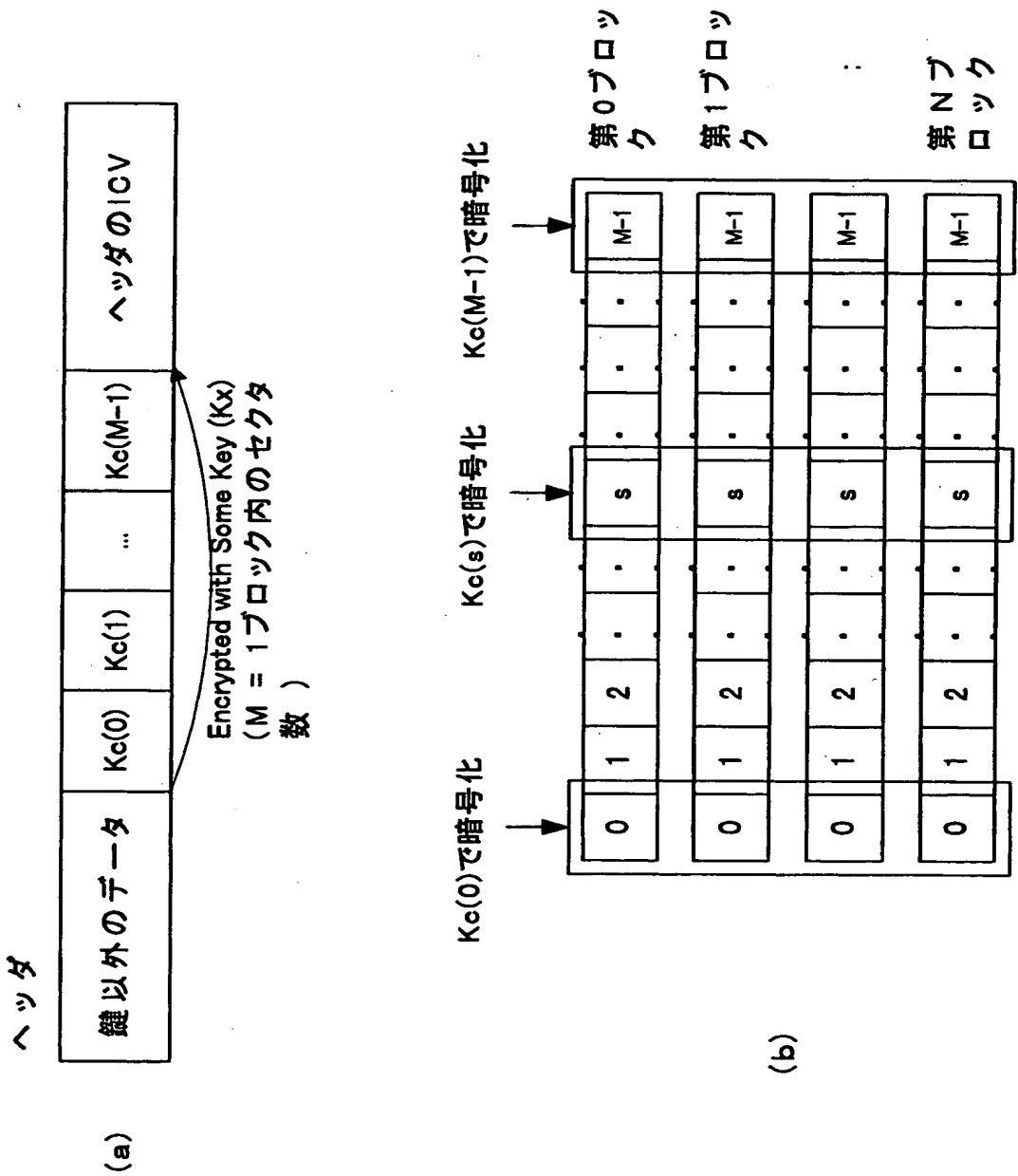
【図25】



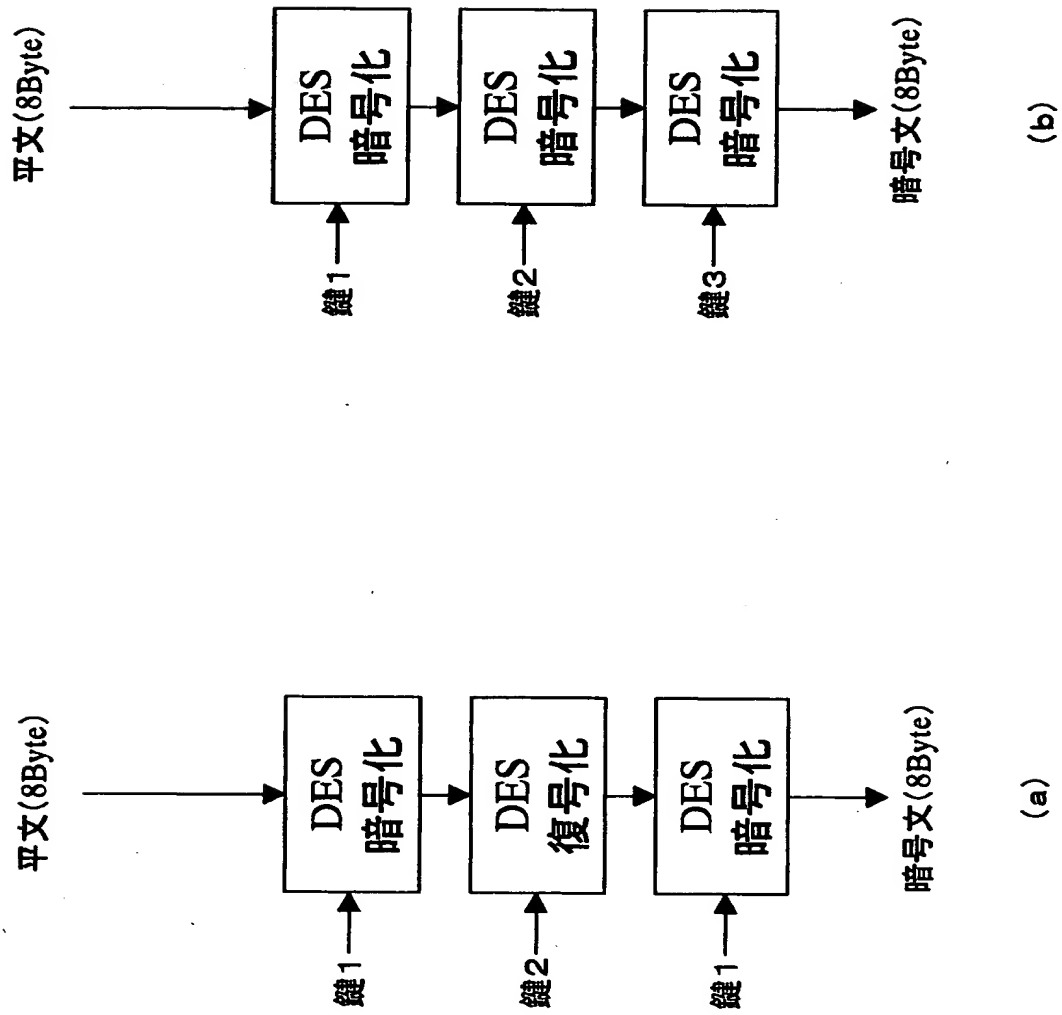
【図 26】



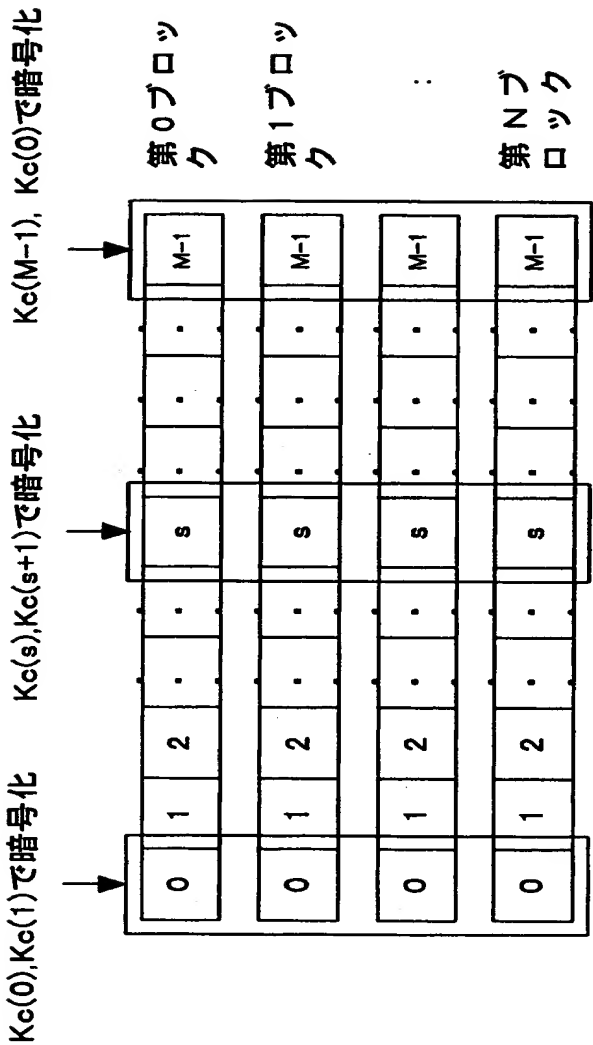
【図 27】



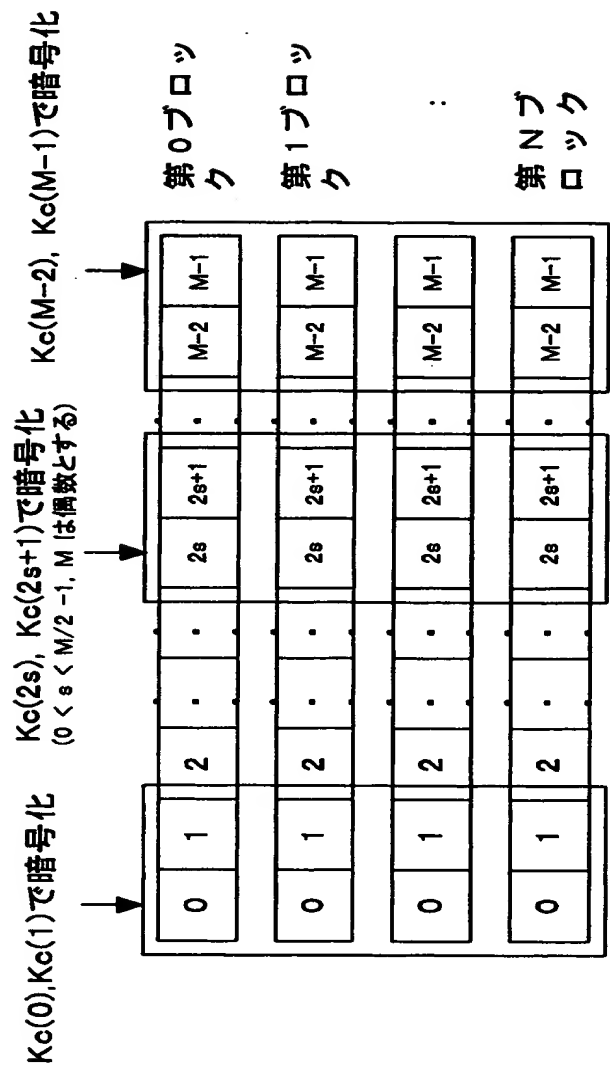
【図 28】



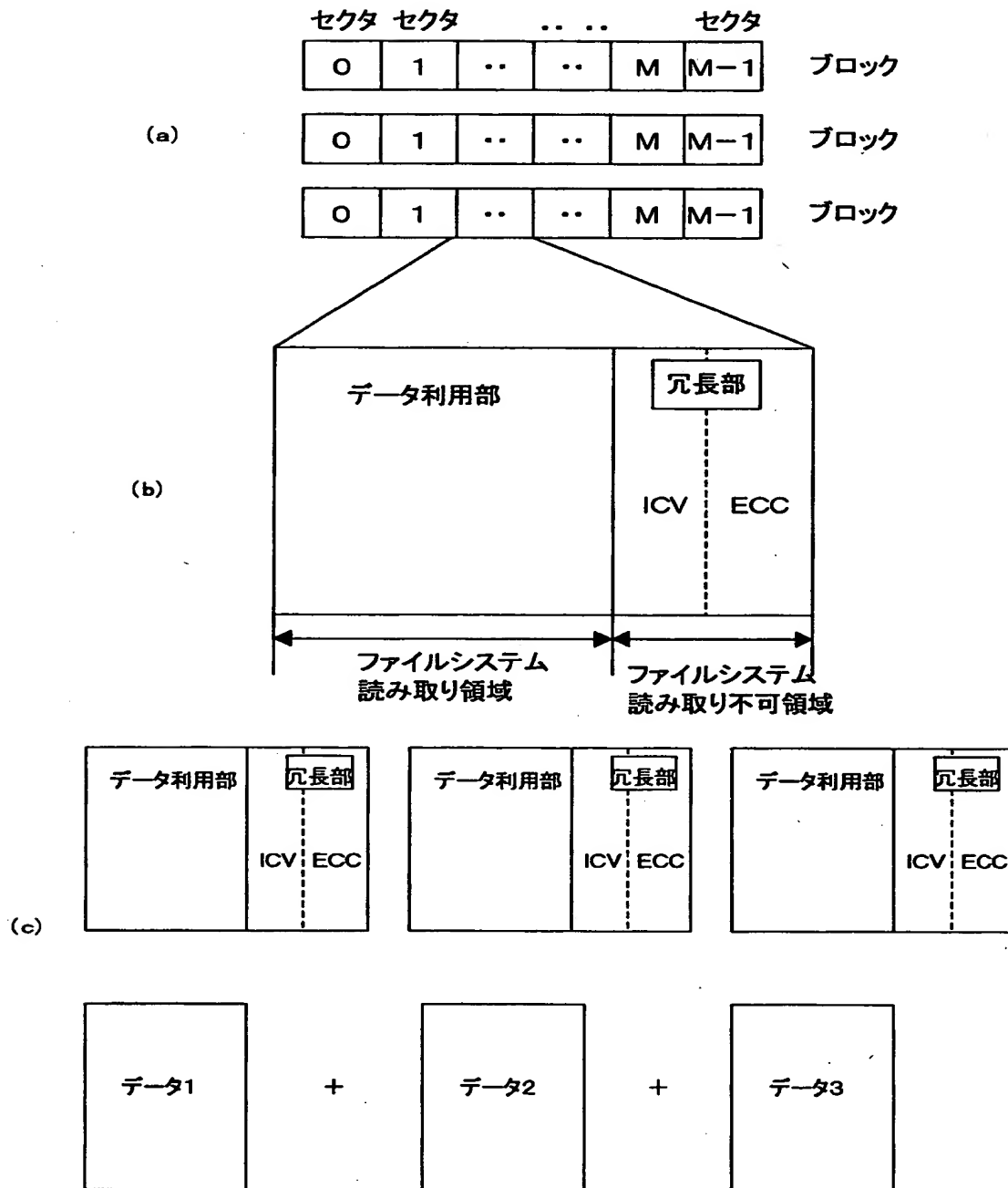
【図 2 9】



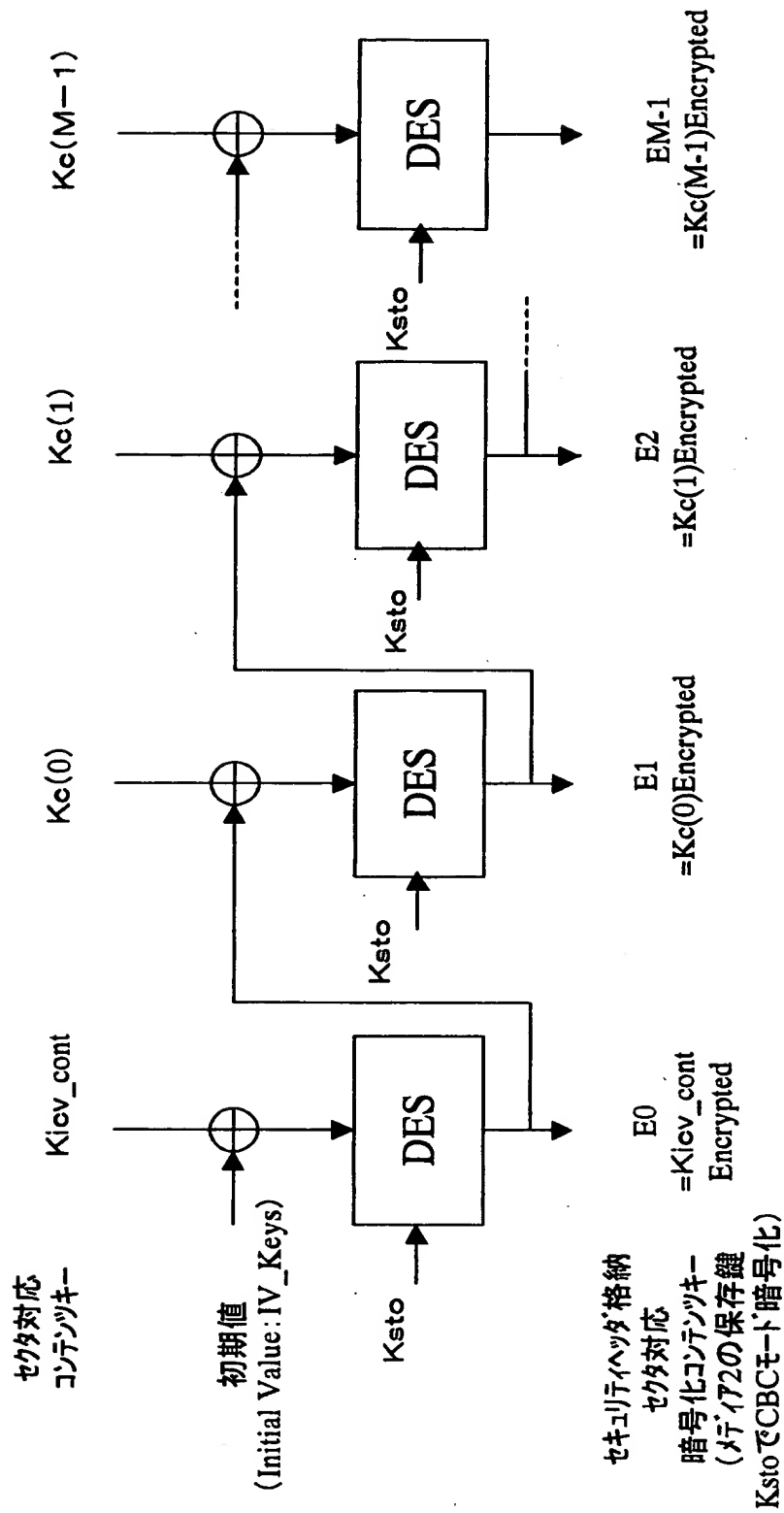
【図 30】



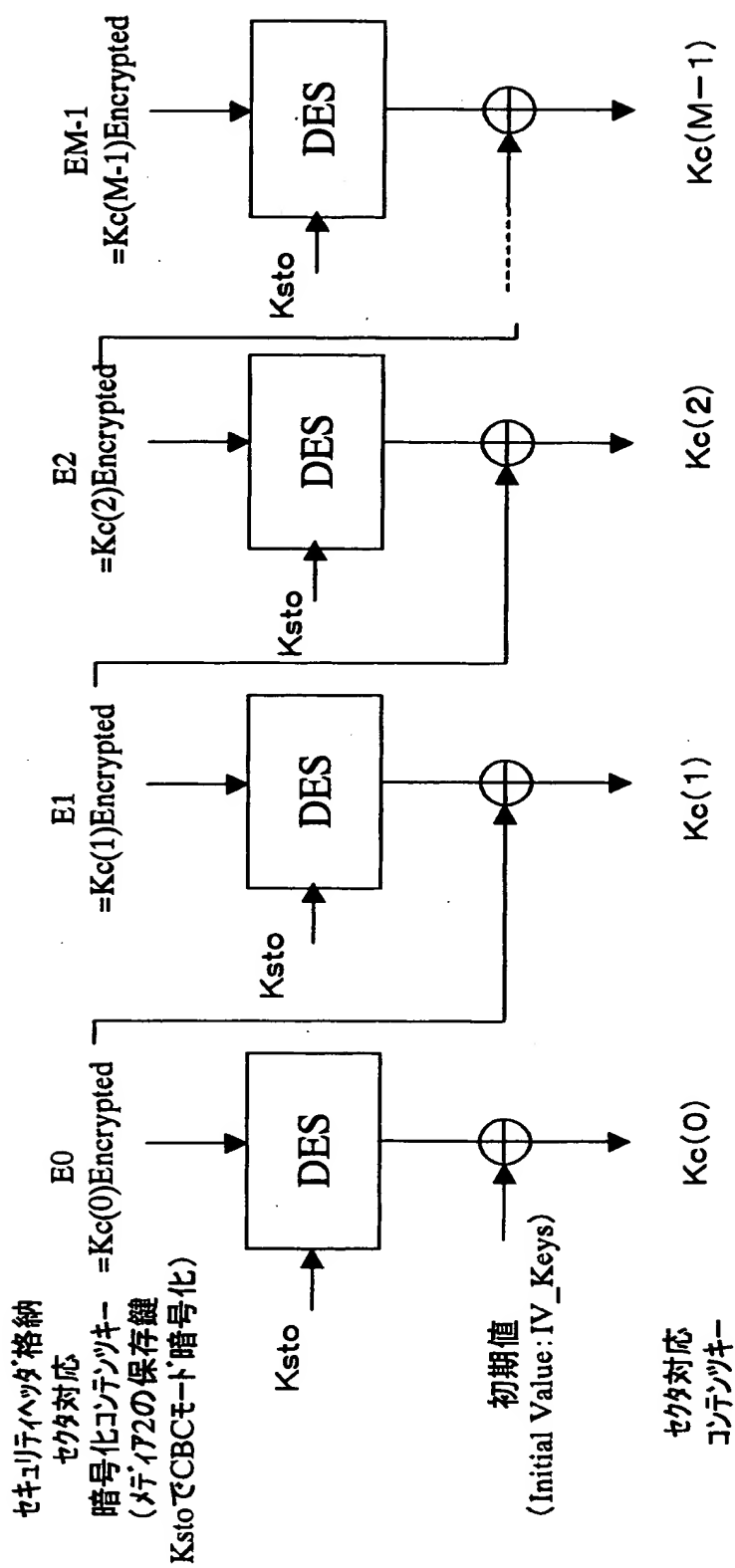
【図 3 1】



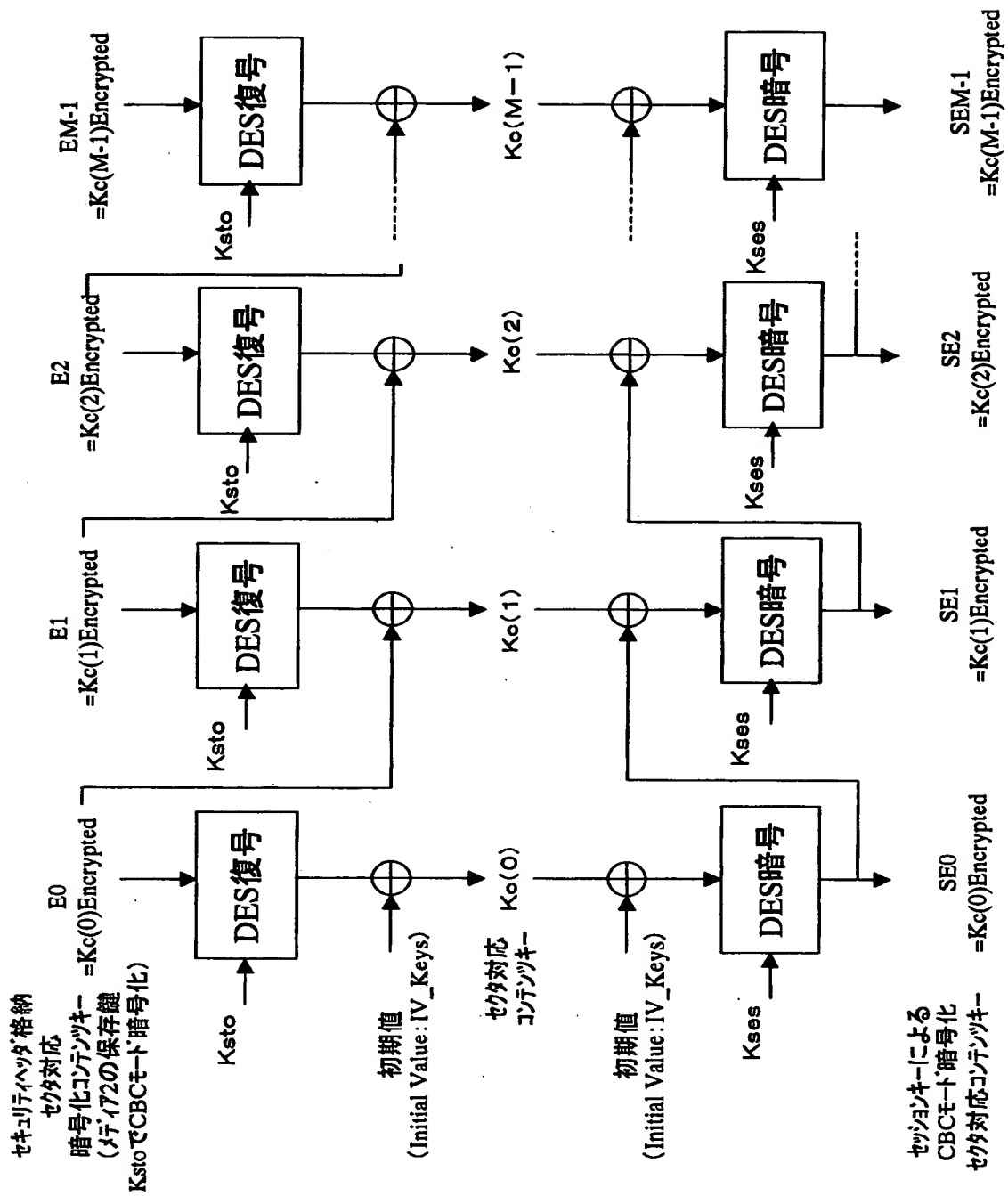
【図 3 2】



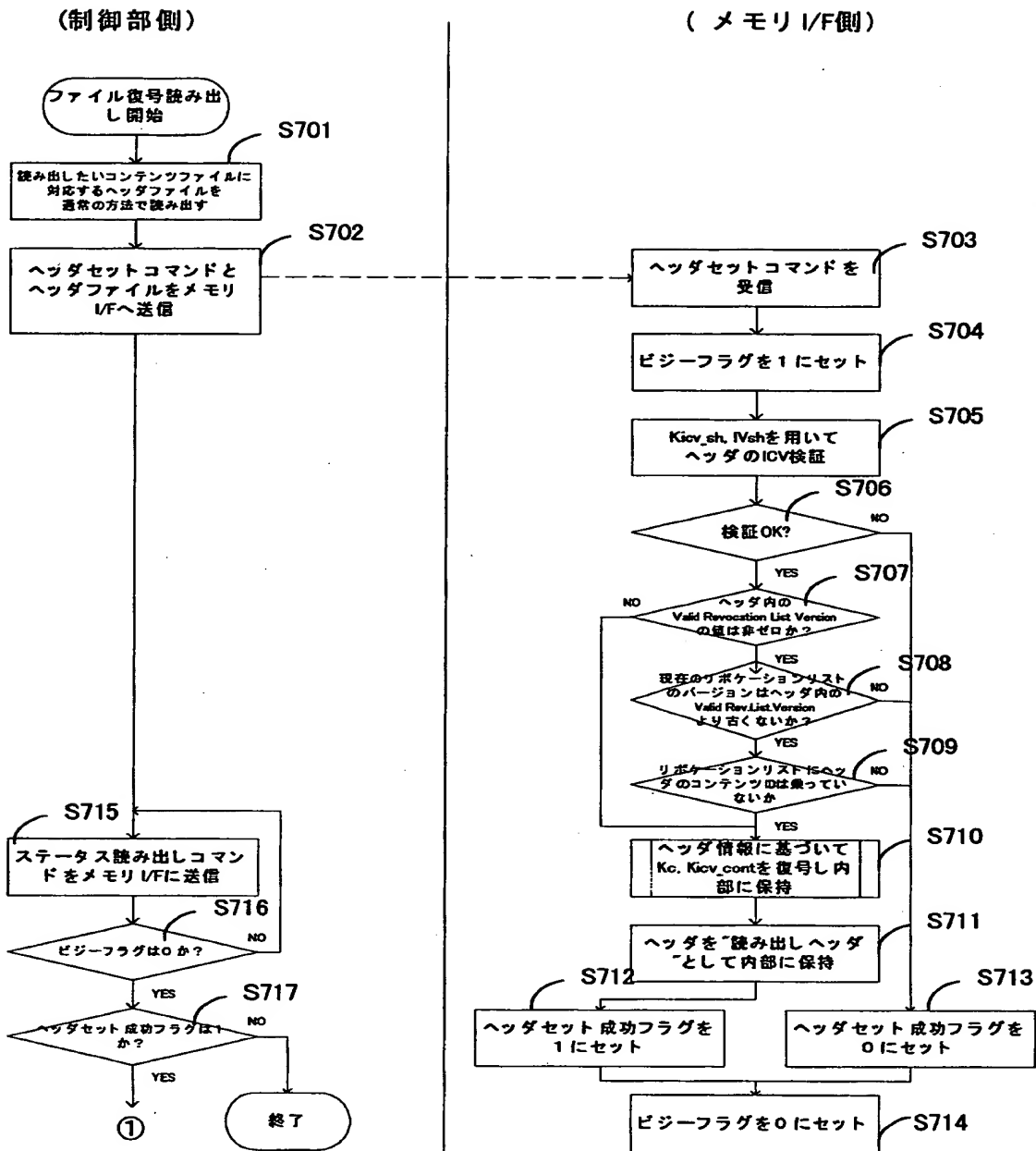
【図 33】



【図 34】

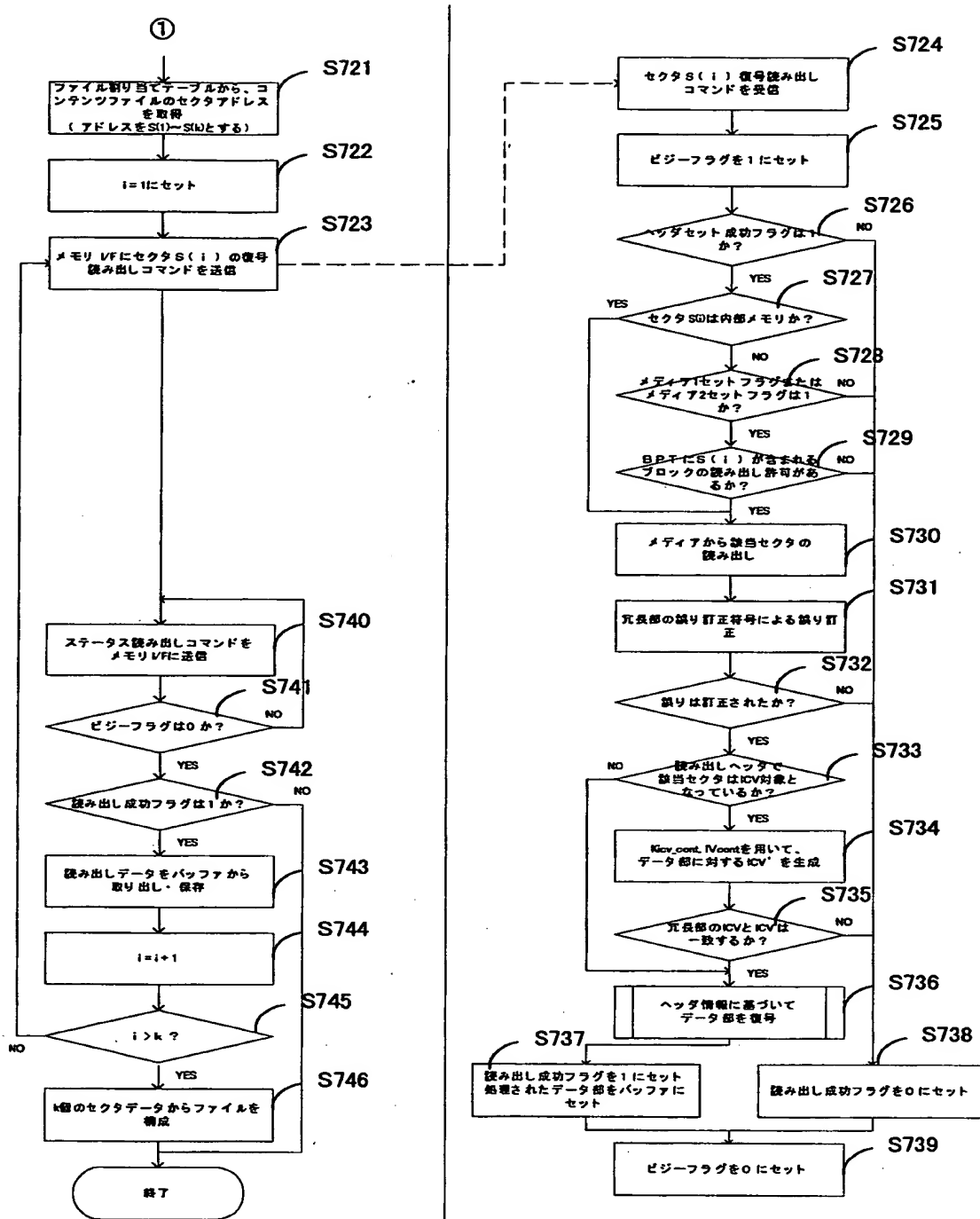


【図 35】



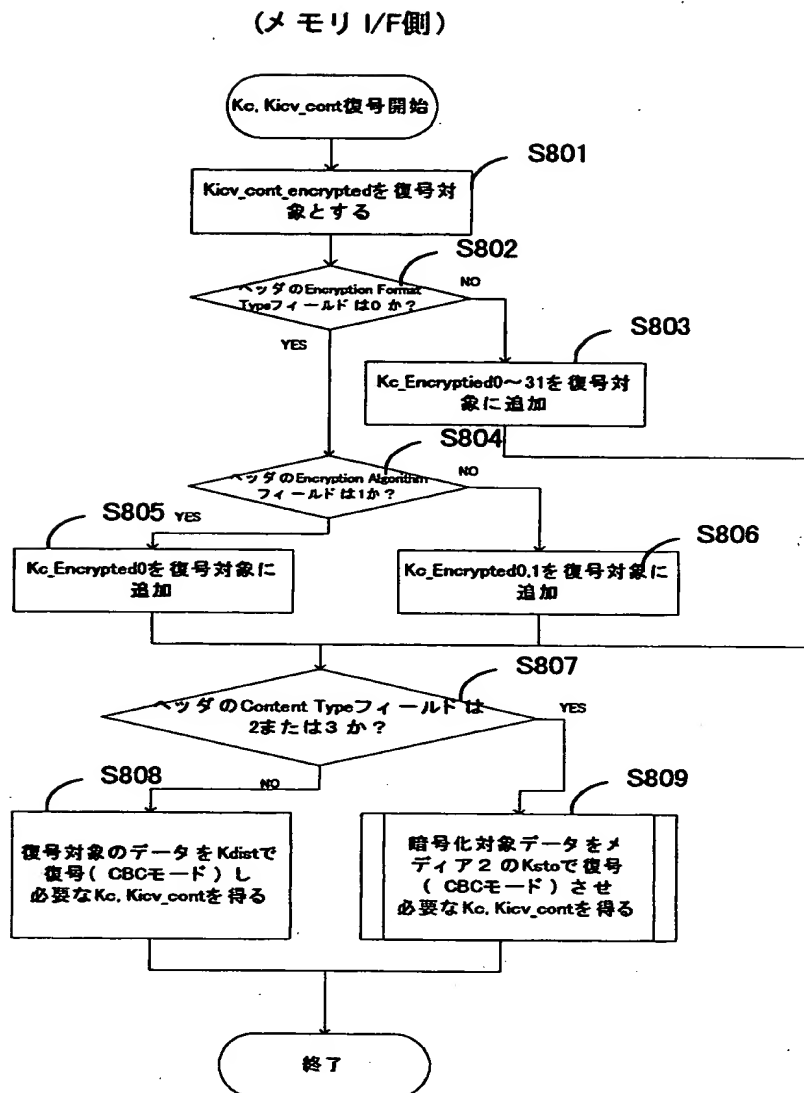
ファイルの復号読み出し処理

【図 3 6】



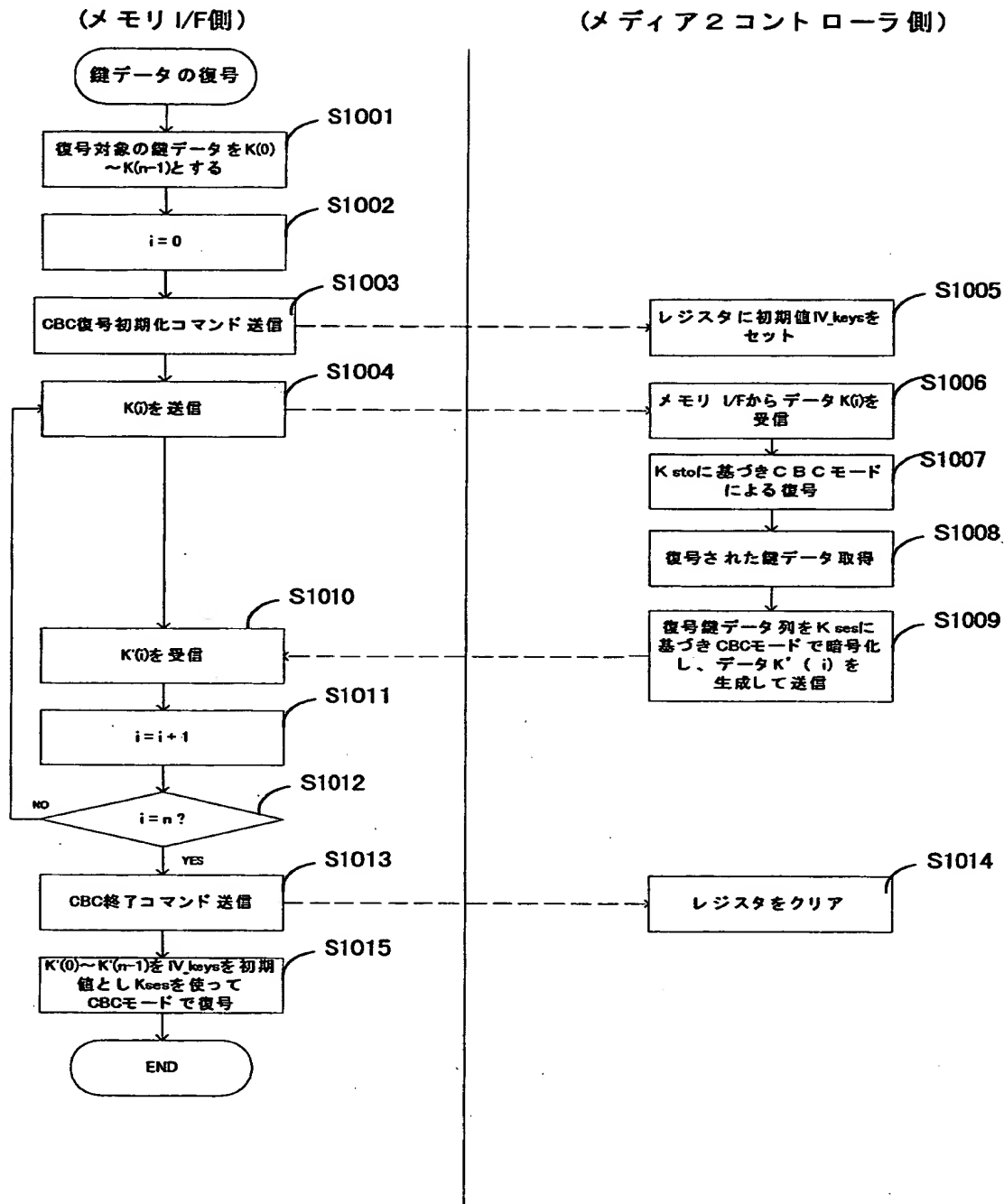
ファイルの復号読み出し処理

【図 37】



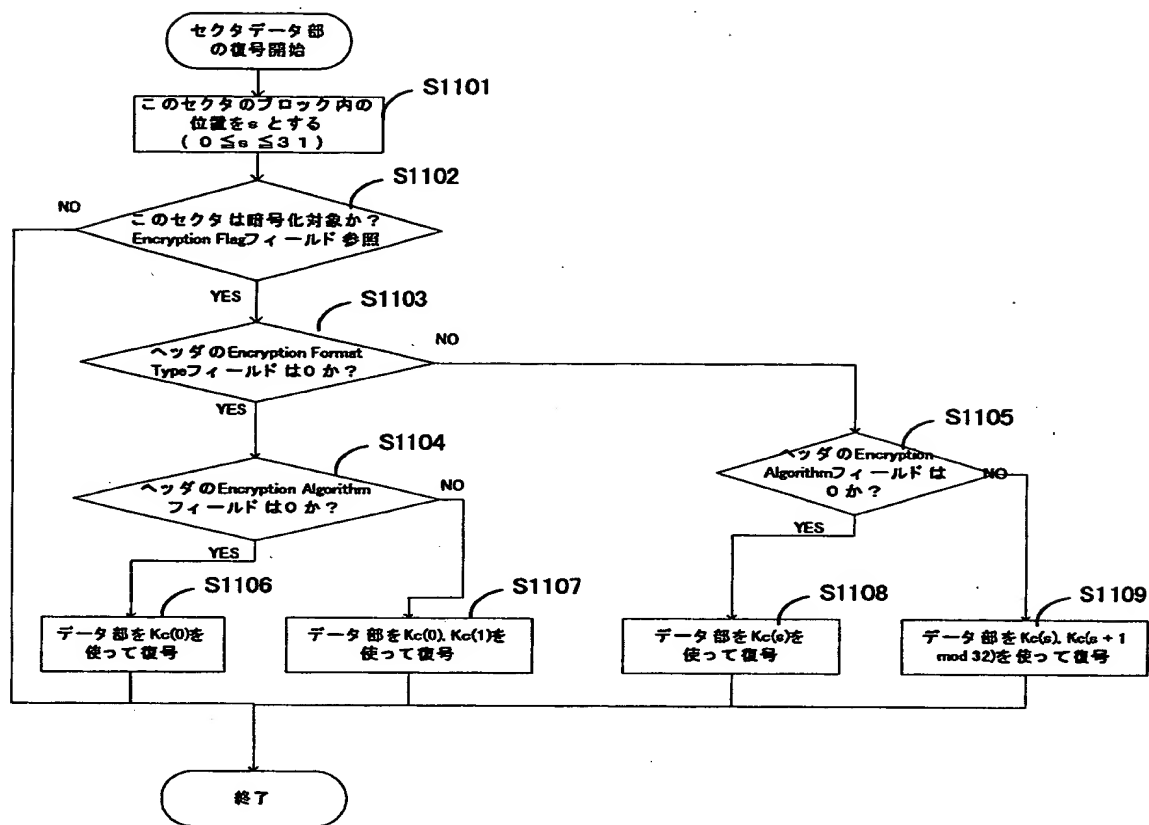
フロー 4-3 : Kc, Kicv_contの復号

【図 38】



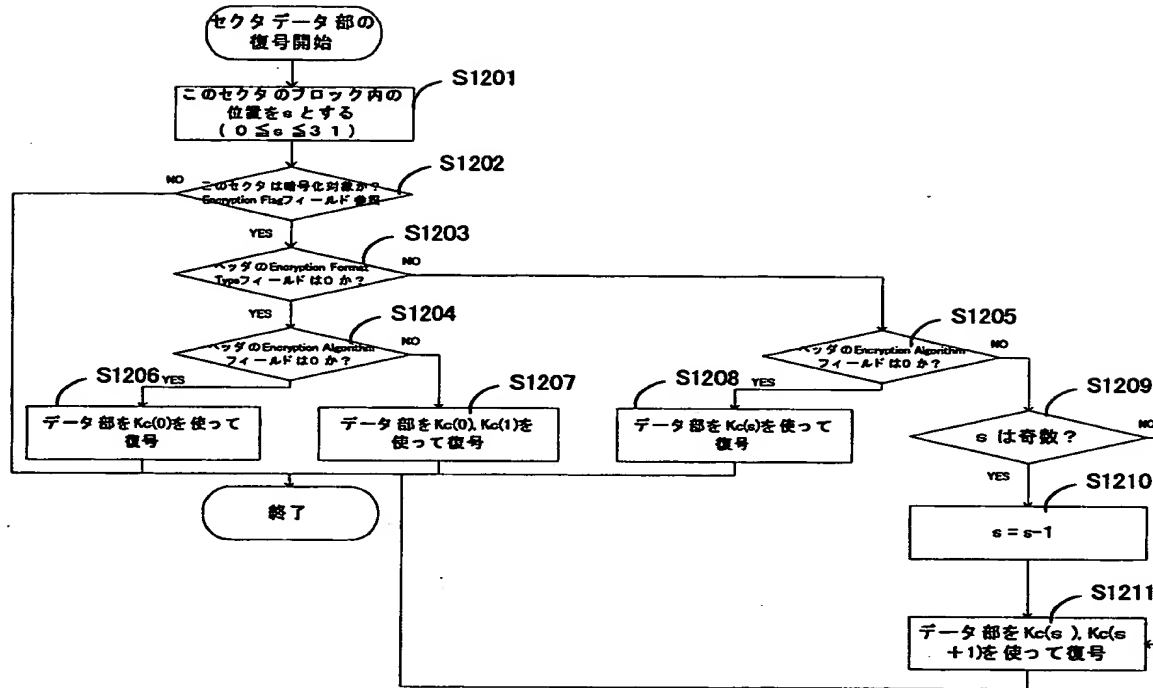
復号対象データをメディア2のKstoで復号

【図39】



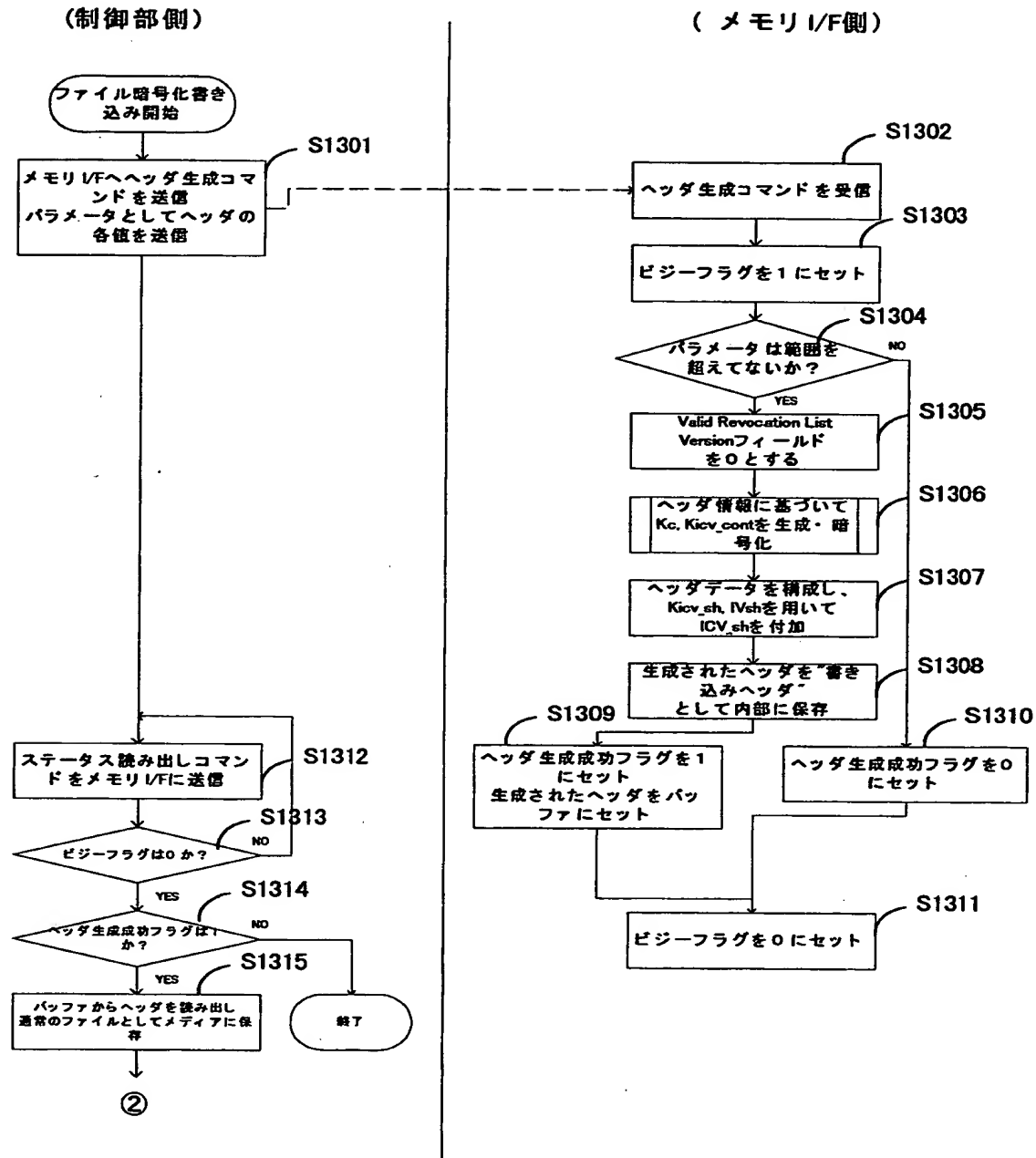
セクタデータ部の復号(その1)

【図 40】



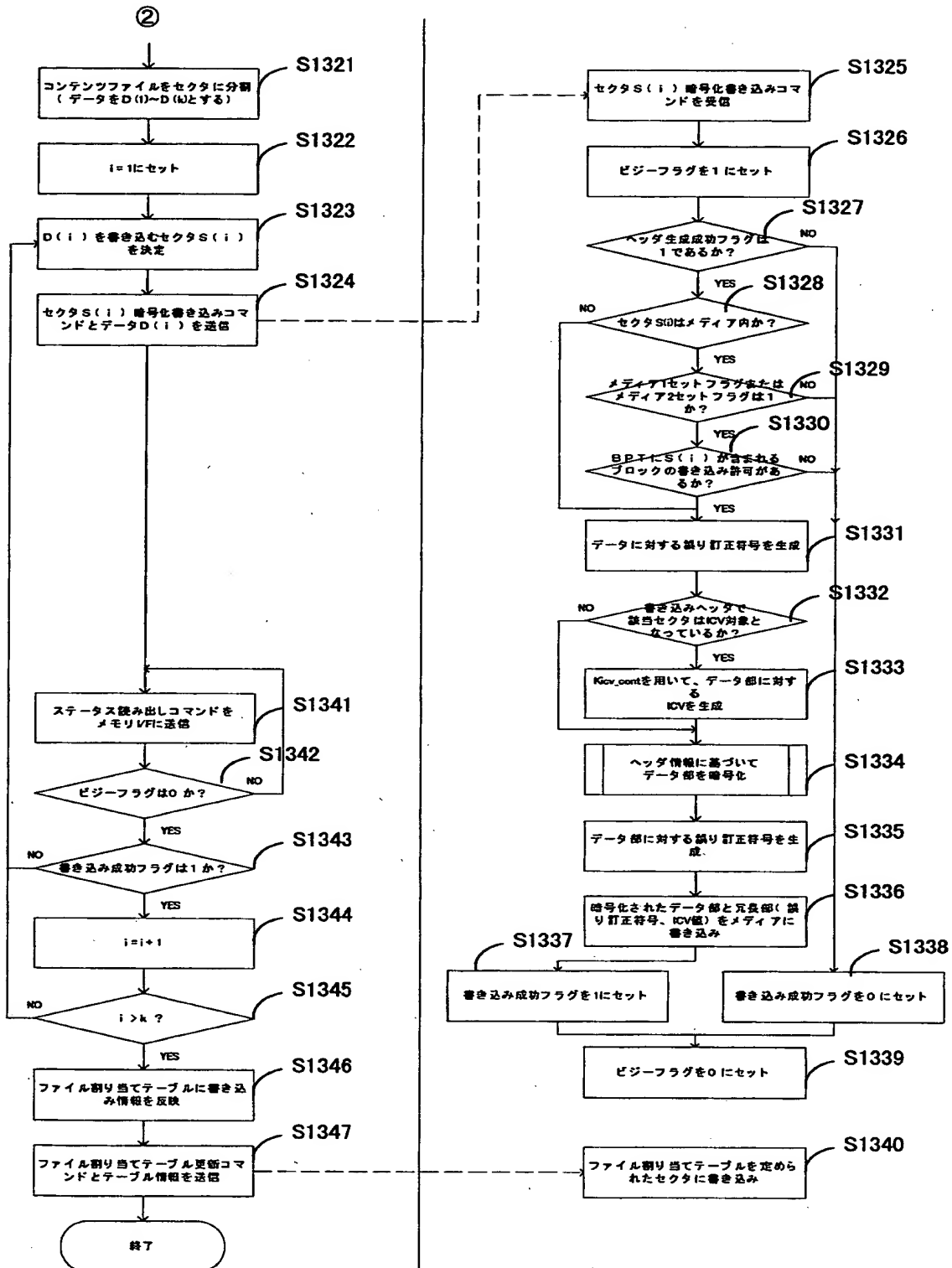
セクタデータ部の復号(その2)

【図 4 1】



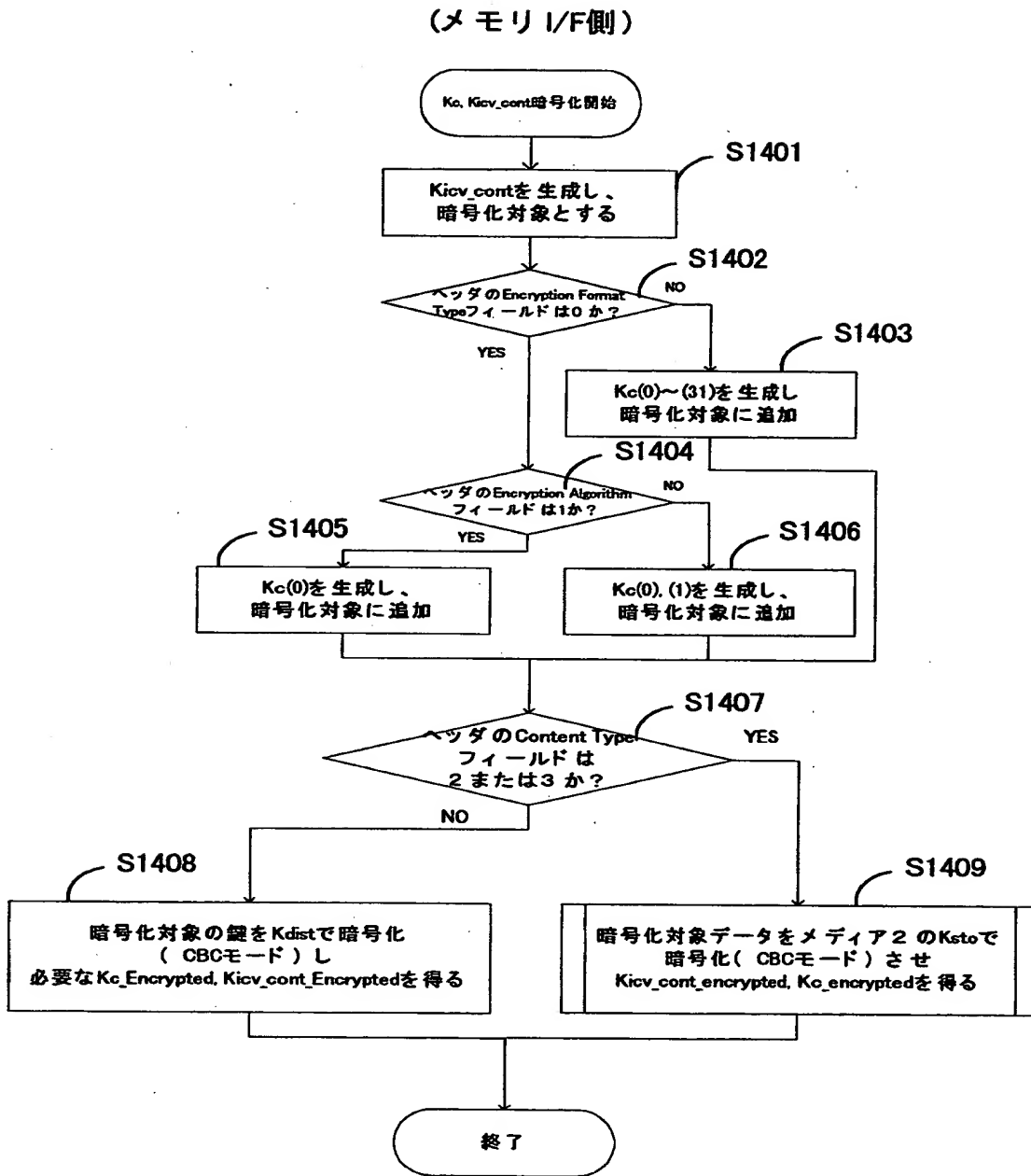
ファイルの暗号化書き込み処理

【図42】



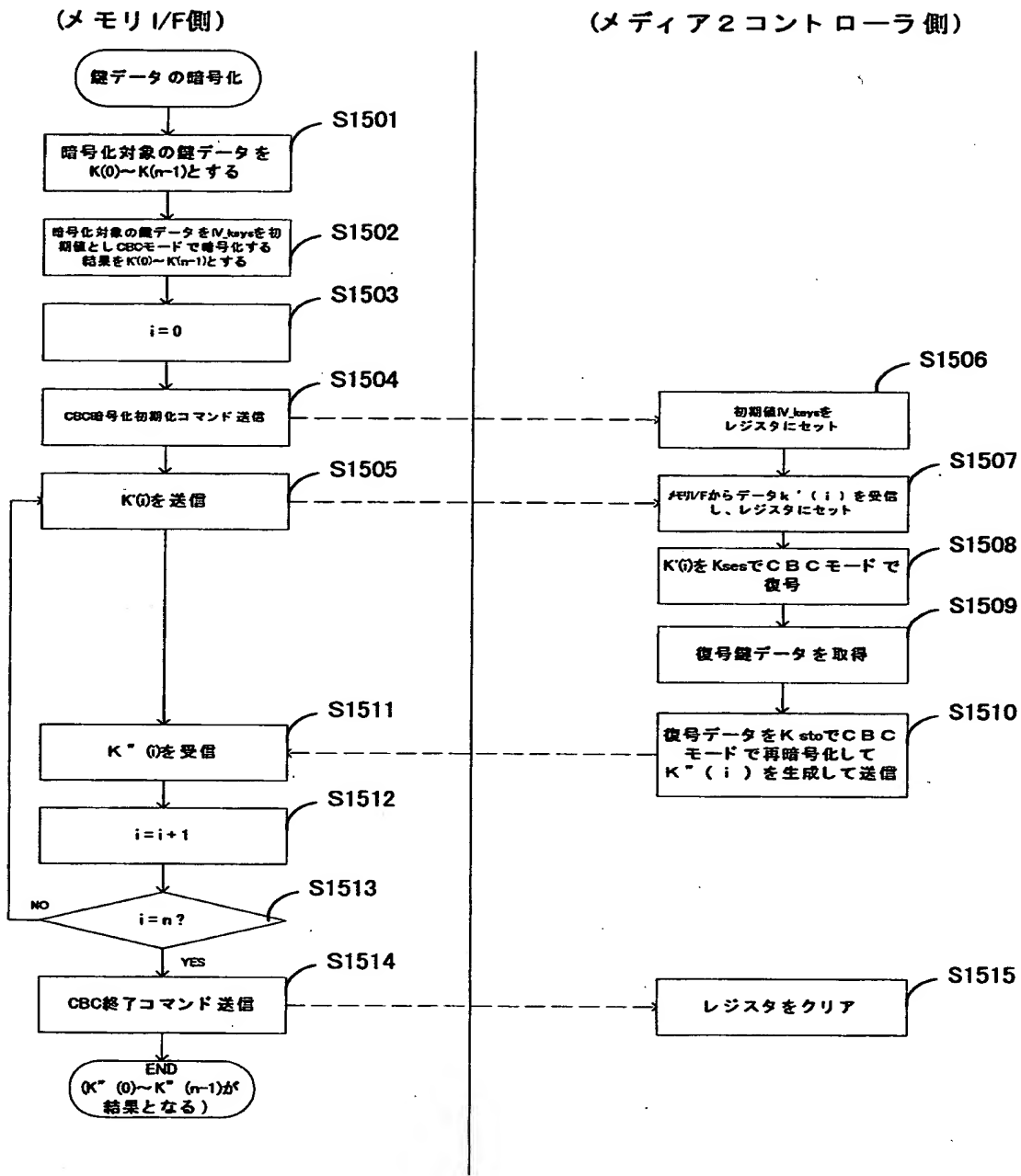
ファイルの暗号化書き込み処理

【図 4 3】



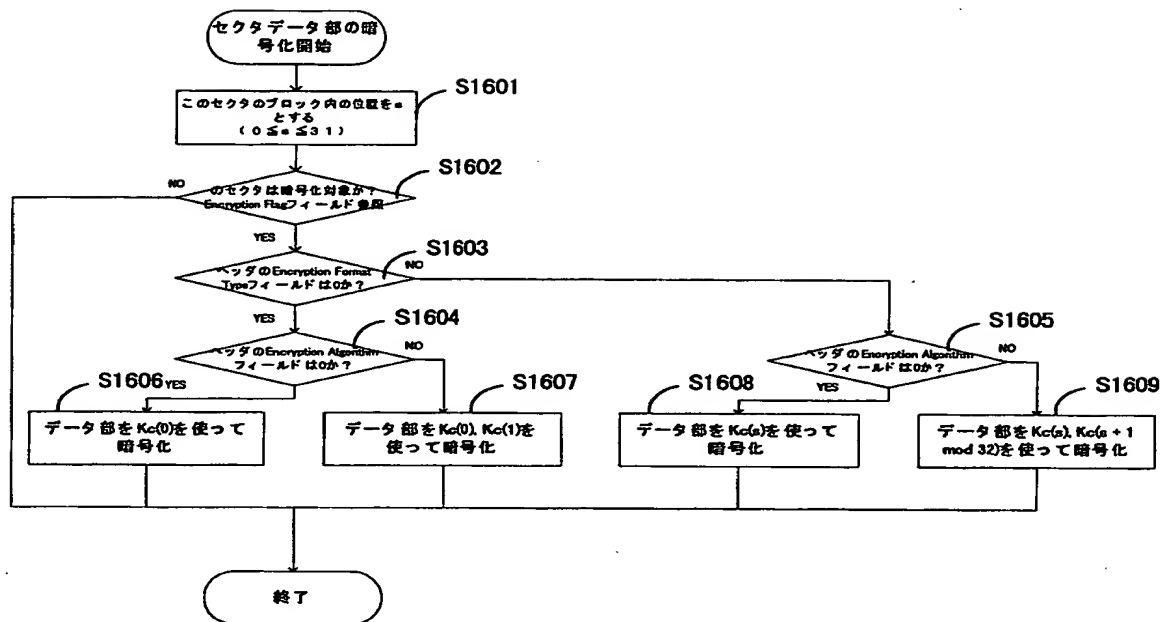
Kc, Kicv_contの暗号化

【図 44】



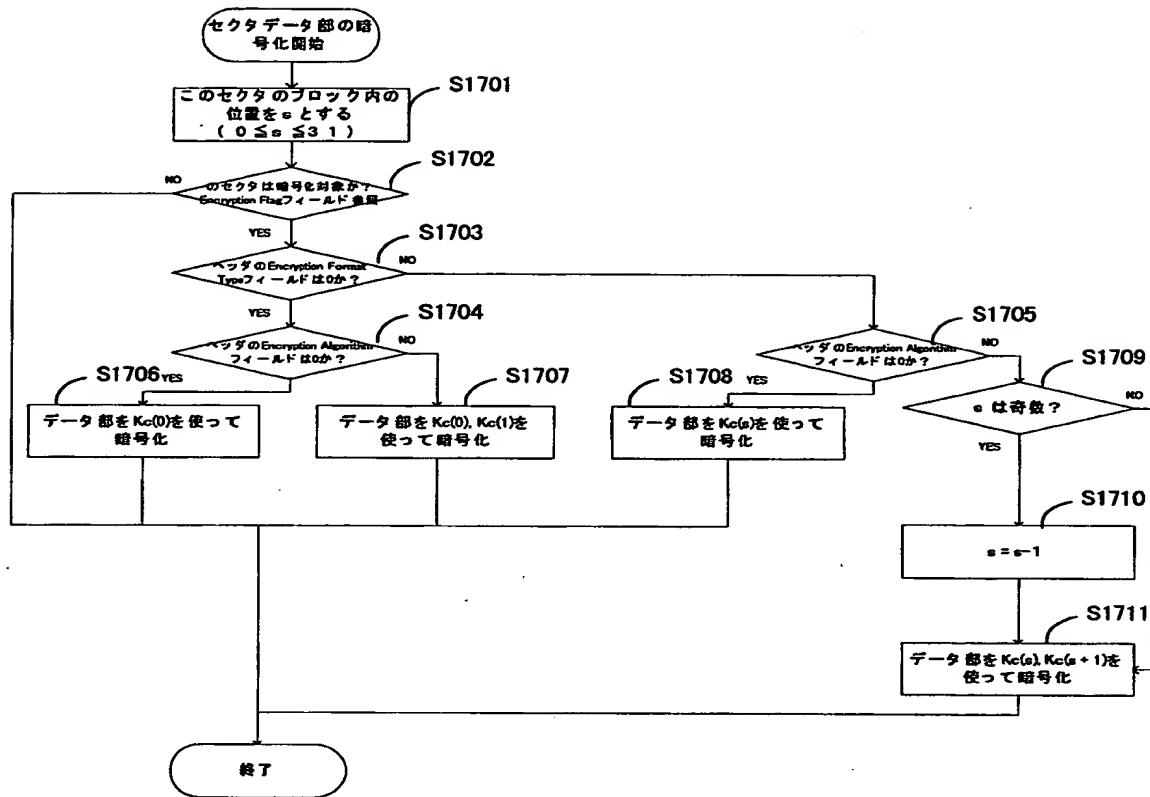
暗号化対象データをメディア 2 の $Ksto$ で暗号化

【図 45】



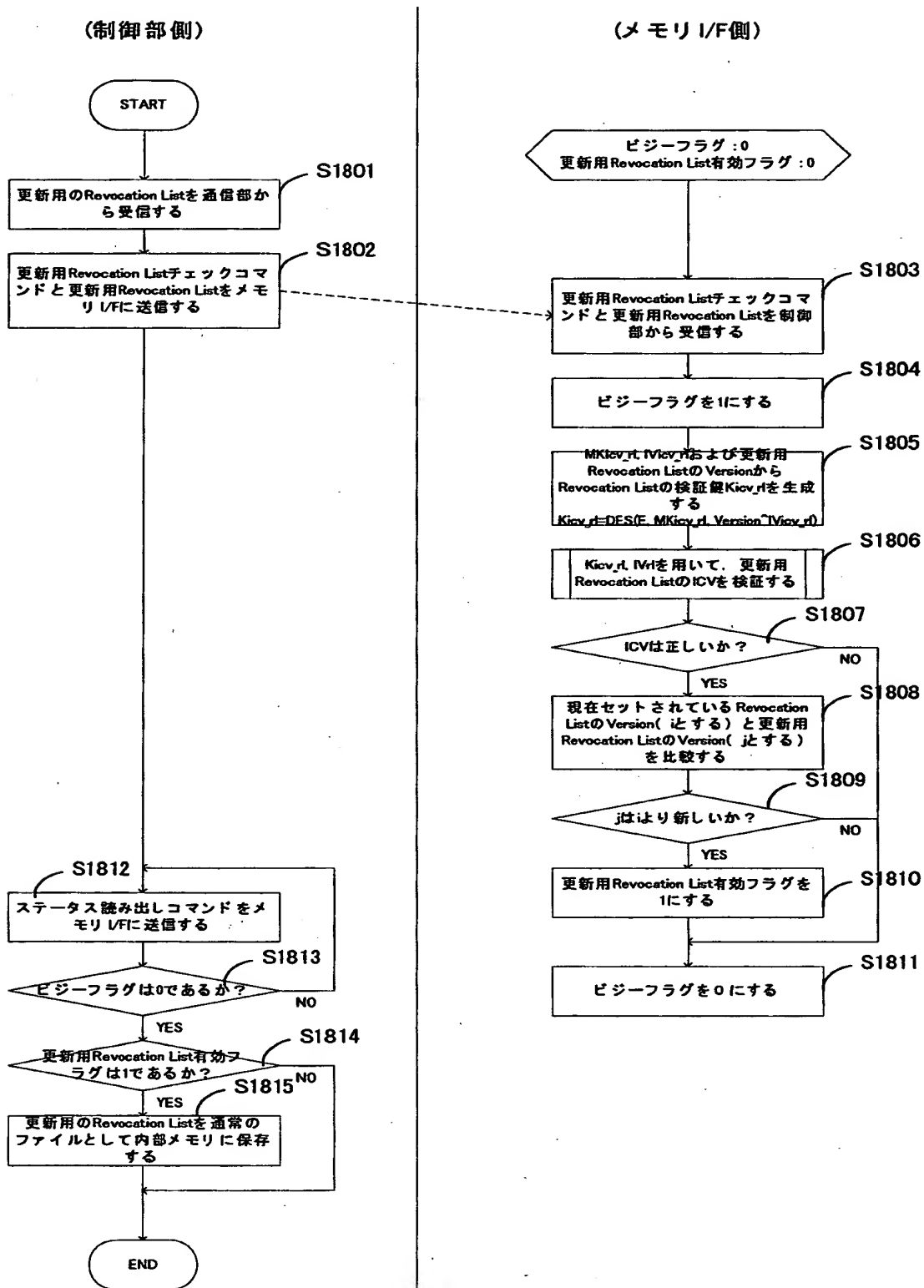
セクタデータ部の暗号化(その1)

【図46】



セクタデータ部の暗号化(その2)

【図 4 7】



Revocation Listの更新

【書類名】 要約書

【要約】

【課題】 記憶手段に記憶するデータの暗号化コンテンツのセキュリティを高め、かつ鍵格納構成を改善した情報記録装置を提供する。

【解決手段】 コンテンツのセクタ対応の複数の暗号鍵について、データ記録再生装置とデータ記憶装置間においてCBCモードでの暗号化処理を実行する。CBCモードで暗号化された結果のデータをコンテンツに対応するヘッダに格納する構成とした。CBCモードによる鍵の暗号化処理は、コンテンツを格納するメディアに固有の保存鍵を適用して行なう構成とし、例えばコンテンツ利用時には、相互認証の成立したメディアにおいて鍵データを復号することによってのみ鍵を復号して取得することが可能となり、セキュリティの高い鍵保管が実現される。

【選択図】 図 3 4

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社